UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

OV LOOP, INC., a Delaware corporation, Plaintiff, -v- MASTERCARD INCORPORATED, and MASTERCARD INTERNATIONAL INCORPORATED, both Delaware corporations, Defendants.	)	CIVIL ACTION NO. JURY TRIAL DEMANDED

COMPLAINT FOR VIOLATIONS OF THE SHERMAN ANTITRUST ACT

Plaintiff OV Loop, Inc. ("OV Loop" or "Plaintiff") hereby files this Complaint against Mastercard Incorporated ("Mastercard, Inc.") and Mastercard International Incorporated ("Mastercard International") (collectively "Mastercard" or "Defendants"), and alleges on personal knowledge as to its own acts, and on information and belief as to all other matters, as follows:

I. STATEMENT OF THE CASE

1. This is a federal antitrust action alleging Mastercard's unlawful monopolization and attempt to monopolize interstate commerce through an anticompetitive refusal to deal and denial of access to an essential facility contrary to Section 2 of the Sherman Act, 15 U.S.C. § 2. Mastercard has used exclusionary means to both create and maintain a monopoly in the relevant market and/or to attempt to monopolize the relevant market. It has done so by wrongfully refusing to deal with emerging new technology companies such as OV Loop because, as Mastercard itself states in United States Securities and Exchange Commission filings, such new technology threatens to disintermediate Mastercard's business. Mastercard has done so in large part through selective access to its Mastercard Digital Enablement Service ("MDES") tokens, which it provides

for mobile wallets like Apple Pay, Google Pay, and Samsung Wallet. These tokens are required for any company to compete in the mobile wallet payment business. Mastercard is the token service provider ("TSP") for its branded cards, *i.e.*, it provides tokens for banks that issue its cards. Through this position, Mastercard, not the issuing bank or the cardholder, controls which mobile wallets can host, for example, a consumer's Citibank or Bank of America Mastercard. Mastercard exercises this control through a certification process, and, in turn, has weaponized its exclusionary power to enforce its monopoly power, disabling emerging threats like OV Loop.

2. Mastercard refuses to deal with OV Loop, directly excluding OV Loop from the First Relevant Market, defined below. Mastercard further refuses to provide OV Loop with equal access to Mastercard's MDES. There is no benign reason for Mastercard to so exclude, and, indeed, Mastercard's of-record excuses are purely pretextual.

3. OV Loop's mobile wallet is part of OV Loop's "super-app." Unlike mobile wallets Mastercard has certified, which are not super-apps, OV Loop has the only mobile payment application that is platform agnostic. This means its platform universally works across iPhones and Android phones alike, allowing users to tap-to-pay at more locations than Apple Pay, Google Pay, and Samsung Wallet combined. Certifying OV Loop would generate money for Mastercard in the near term, as it would mean more Mastercard cardholders would consummate more Mastercard transactions. In the credit card business, volume is all. More consumers would carry Mastercard branded cards, providing Mastercard with higher revenue and margins in mobile wallet transactions.

4. Mastercard stands in the way of progress for a reason: Mastercard is choosing to sacrifice short-term revenue in order to gain long-term anticompetitive advantage. It does so to ensure that the OV Loop super-app platform cannot reduce Mastercard's monopolistic pricing

power through the disintermediation of Mastercard's business. By denying OV Loop Mastercard's MDES certification, Mastercard is able to keep OV Loop from gaining traction among consumers and merchants and ultimately, to prevent OV Loop from offering point-of-sale ("POS") payment methods that use non-card network payment rails with lower transaction fees. Mastercard believes that OV Loop is a threat to Mastercard's business model because OV Loop's platform can facilitate consumer mobile wallet payments to merchants through not just branded credit cards, but also other payment methods, such as payments directly from a consumer's bank account. This type of transaction carries substantially lower fees than the fees charged by Mastercard for the same transaction. If a mobile wallet with alternative payment rail capability were to gain traction among consumers and merchants, this solution's alternative payment rail option, which carries lower transaction fees than its branded card option, would take market share from Mastercard. Many merchants would certainly offer lower prices for purchases made with alternative payment methods that impose lower fees to avoid payment methods that require merchants to accept high and unnecessary transaction costs. Other merchants would simply decline to take the more expensive branded card payment option, while offering consumers lower-priced goods and services reflective of the merchant's cheaper super-app-alternative rail transaction costs.

5. To avoid competition, Mastercard restricts customers to a handful of mobile wallets that do **not** offer, and are not positioned to offer, alternative rail payments, *i.e.*, Apple Pay, Google Pay, and Samsung Wallet. This protects Mastercard's ability to charge supracompetitive fees on each transaction. Mastercard's behavior limits competition within the relevant market, stifles innovation, restricts consumer ability to choose a mobile wallet other than Apple Pay, Google Pay, or Samsung Wallet, and increases costs to merchants and consumers.

6. To put these allegations into historical context: Debit and credit card transactions

via Apple Pay, Google Pay, and Samsung Wallet have grown exponentially over the past few years. These applications are known as "mobile wallets," and with them, in-person payments no longer require a physical card. Tap-to-pay mobile wallet transactions in the United States—where the customer presents a mobile wallet on their mobile device to pay at a physical point of sale—are almost exclusively delivered by Apple, Google, and Samsung contactless mobile wallets. The Apple, Google, and Samsung mobile wallets are siloed in their walled gardens and **not** "universal." For example, a consumer cannot use their Apple Pay wallet if they switch to an Android phone, nor can they use their Samsung Wallet if they switch to an iPhone. Thus, unlike in China and other countries, where universal wallets like the WeChat Pay super-app lets consumers pay virtually anywhere with **any** phone they choose, there is no universal wallet in America. This is primarily due to TSPs like Mastercard, which control the mobile wallets of their choosing to allow bank credentials to be provisioned to, thereby controlling the mobile wallet market, the emergence of new mobile payment platforms, and the pricing for mobile payment transactions.

7. Mastercard is one of the two leading payment card networks in the United States. Visa is the other predominant network. Mastercard and Visa fix the "interchange" transaction fees charged by issuers (banks that issue cards under the card network brands (*e.g.*, Mastercard, Visa)) and processors to merchants. Their anti-competitive behavior has been well documented, and the interchange fees charged by the card networks total billions of dollars every year; indeed $161 billion in 2022. These fees affect **every** purchase made with a credit or debit card, including those made with mobile wallets.

8. There has been a massive increase in processing fees over the last ten years, more than doubling over the past decade, and soaring 16.7% last year to an all-time record high of $160.7 billion. Merchants paid $126.4 billion in processing fees for credit card transactions in 2022, an

increase of 20%. *See* https://www.supermarketnews.com/consumer-trends/retailers-paid-1264b-credit-card-processing-fees-2022. Interchange fees for Mastercard's and Visa's credit cards, which dominate the market, increased 21% to $93.2 billion, representing a majority of the processing fees incurred within the United States. *Id.* Strikingly, swipe fees are most merchants' highest operating costs after labor and drive-up prices paid by consumers. *Id.* In 2022, credit and debit card swipe fees cost the average household an estimated $1,024 in higher prices; the first time the number topped the $1,000 mark. *Id.* This matters. Most of these fees are paid by the merchants to the card-issuing banks and the payment card networks. These fees are, perforce, eventually pushed down to the consumer. The merchants pay them in the first instance, but then pass much of the transactional overhead to the customers. **These processing fees are a tax on commerce, a tax on merchants, a burden on consumers, and sand in the gears of the United States economy.**

9. High transaction fees contributed to a net profit margin of 45% for Mastercard, as contrasted with the general retail average net profit of 2.4%. Over the same period, the networks' costs have not increased nearly proportionately. In 1966, Mastercard started as the Interbank Card Association (ICA) to facilitate credit card transactions for member banks. By 2005, as an association working for banks, it, through its payment rails, operated like a powerful utility with market power, enjoying net income in the hundreds of millions and a profit margin of roughly 13%. In 2006, after it became an independent for-profit public company, its profit margins exploded to roughly 45% while its net income grew from $229 million to a whopping $12.264 billion by 2022. *See* https://en.wikipedia.org/wiki/Mastercard. From June 1, 2006 to January 25, 2024, Mastercard's stock prices have grown over 93 times — this is a larger growth than 99% of all other publicly traded stocks in the entire stock market during this period, including Apple,

Alphabet (Google), Meta (Facebook), and Amazon.

10. Mastercard operates a payment card network over which merchants can route card transactions via POS devices connected to the network. Mastercard also operates as a TSP that generates security tokens for Mastercard branded cards for use in digital payment transactions, including tokens saved on mobile wallet devices and used by mobile wallet applications.[1]

11. Specifically, when a cardholder loads a credit or debit card into a mobile wallet, the card is "tokenized," meaning the original personal/primary account number ("PAN") printed on the card is replaced with a different PAN number—the "token" or tokenized PAN—to protect the original PAN during stages of a debit/credit transaction. The TSP that generates the token also maintains a "token vault" that stores and matches the original PAN corresponding to each token. When the cardholder initiates a transaction using a mobile wallet, the merchant receives only the token and a unique cryptogram, not the original PAN. The merchant sends this token and cryptogram to the acquirer, which sends the token to a network for processing. To complete the transaction, the TSP must "detokenize" the token, which involves converting the token to its associated original PAN stored in the token vault.

12. Mastercard, a TSP, controls Mastercard's tokens, generated by MDES, regardless of the owner of the mobile wallet. **Only companies approved by Mastercard can request and**

[1] The terms "tokenization" and "token" are used somewhat confusingly in the industry. For example, sometimes these phrases refer to the process of obfuscating the original payment card number, *i.e.*, the original/funding personal account number, and the resulting data used in the conventional data's stead (*e.g.*, a tokenized personal account number), while at other times it refers to that process (and result) combined with the provisioning of cryptographic keys (keys used to encrypt data) to use in generating cryptograms (encrypted data used to make an authorization decision), while in yet other instances it is used to refer to the generation of cryptograms and the cryptograms themselves. Here, the terms "tokenization" and "token" will be used, respectively, to refer to the process of obfuscating the original payment card number and the resulting data used in the conventional data's stead (*e.g.*, a tokenized personal account number), unless otherwise noted.

receive Mastercard MDES tokens for a mobile wallet. Approved mobile wallet providers that can receive MDES tokens are called Token Requestors ("TRs"). Absent Mastercard approval, a third party cannot offer a mobile wallet that processes Mastercard MDES tokens and so cannot offer a wallet that can host a consumer's Mastercard cards. In short, Mastercard's tokenization service is now an essential facility for processing Mastercard mobile contactless payment transactions: absent Mastercard certification, explained below, the third-party wallet provider cannot process digital wallet transactions. Since virtually all Mastercard branded card programs now rely on Mastercard MDES to provision tokens to various mobile wallets or TRs, Mastercard has become a powerful gatekeeper to determine which companies can become a TR to allow their users to access Mastercard MDES tokens for mobile contactless payments.

13. For traditional payment card transactions, Mastercard typically receives roughly five bps (five basis points per transaction equates to 0.05%). Similar to traditional card transactions, Mastercard receives an interchange fee from each transaction consummated through mobile wallet tokenized contactless payment.

14. For years, and as alleged in detail below, Mastercard has erected anticompetitive barriers to entry, and has consistently foregone short-term profits for longer-term anticompetitive gain, to acquire/maintain its monopoly in, and/or attempt to monopolize, the United States consumer-merchant mobile contactless payment wallet network processing market.

15. As a recent case in point, Mastercard, Visa, and Apple have been sued in an antitrust class action, *Mirage Wine and Spirits Inc. v. Apple, Inc., Visa Inc. and Mastercard Incorporated*, No. 3:23-CV-3942-DWD (S.D. Il.) (case initiated Dec. 14, 2023). This complaint alleges, in great detail, an illicit agreement amongst the three to restrain trade. Put bluntly, the named plaintiff alleges that Mastercard and Visa essentially bribed Apple to ensure that Apple Pay would not

emerge as an alternate network—a payment not to compete. Apple's revenue of 15 bps under this non-compete covenant is substantial.

16. This is not an anomaly. Over the decades, Mastercard has been found to abuse its market power through exclusionary practices, all to create supracompetitive margins, as set forth below.

17. Mastercard lets certain companies use its MDES token services, including Apple, Google, Samsung, LG, and Garmin for Apple Pay, Google Pay, Samsung Wallet, LG Pay, and Garmin Pay, respectively. It will work with these companies because they do not threaten to disintermediate Mastercard's core business, as set out below. These companies' primary businesses are to sell more phones, devices, or ads under their own walled gardens, which are not designed to become universal wallets that work across devices and operating systems.

18. But Mastercard refused to work with OV Loop. OV Loop was founded and funded to create a super-app platform, *i.e.*, a unified commerce platform with a universal wallet, mail, and messenger app for buyers, and an omnichannel payments, rewards, and engagement tool for sellers. As set forth below, a super-app platform is a new digital, mobile platform which enables numerous online functions, principally including consumer-merchant payments, engagement, and loyalty. These new payment methods can provide multiple tender types, including Mastercard and Visa payment processing networks, **and** alternative tender types that bypass Mastercard and Visa networks. Super-apps in countries like China, India, and Brazil use alternative payment rails such as bank-account-to-bank-account real-time payments and other tender types that do not go over card network rails and so provide significantly lower transaction fees. These super-apps have no need for Mastercard. They do not pay the massive Mastercard processing fees; nor do merchants and their consumer customers.

19. A super-app is terrific for the consumer and the economy. But Mastercard perceives these apps as bad, even though a super-app can help transition credit and debit card payments from lower-margin plastic card transactions to higher-margin, more secure mobile wallet transactions.

20. Companies in this country are free not to work with competitors. They are free to say no unless they say no for the **wrong** reasons, such as to protect or enhance a monopoly position. A party cannot refuse to deal for the wrong reasons. Motives matter.

21. As explained further below, Mastercard knew full well that OV Loop was founded to build a super-app platform. OV Loop told Mastercard this explicitly and gave presentations to Mastercard that drove the point home. OV Loop demonstrated how it fully satisfies the requirements for MDES certification. Mastercard, however, will not give OV Loop access because the possibility of a payment application using alternative payment rails could threaten its ability to continue charging outrageous transaction fees for mobile wallet transactions. Mastercard believes that a United States super-app would undermine its stranglehold on the consumer-merchant mobile wallet contactless payments network processing services; a market in which it enjoys significant market power, indeed, monopoly power. Mastercard simply refuses to deal with OV Loop without being candid about its motivations or reasons and is sacrificing short-term financial gain for long-term anti-competitive benefit, as alleged in detail below.

22. This is not how competition is supposed to work in this country.

II. THE PARTIES

23. OV Loop is a corporation organized and existing under the laws of the State of Delaware, with its principal place of business at 73 Holton St., Woburn, Massachusetts 01801.

24. Mastercard Inc. is a corporation organized under the laws of the State of Delaware,

with its principal place of business at 2000 Purchase Street, Purchase, New York 10577.

25. Mastercard International is a corporation organized under the laws of the State of Delaware, with its principal place of business at 2000 Purchase Street, Purchase, New York 10577. Mastercard International is a subsidiary of Mastercard Inc.

III. JURISDICTION AND VENUE

26. This is an antitrust action arising under Title 15, Chapter 1 of the United States Code. OV Loop seeks injunctive relief under 15 U.S.C. § 26 and damages under 15 U.S.C. § 15 for Mastercard's violations of Section 2 of the Sherman Act, 15 U.S.C. § 2.

27. This Court has subject-matter jurisdiction under 28 U.S.C. §§ 1331 and 1337.

28. This Court has personal jurisdiction over Mastercard because Mastercard has engaged in systematic and continuous contacts and business activities in this District. Among other things, Mastercard: (a) transacts business throughout the United States, including in this District; (b) has substantial contacts with the United States, including in this District; and/or (c) is engaged in an illegal anticompetitive scheme that is directed at and has the intended effect of causing injury to persons residing in, located in, or doing business throughout the United States, including in this District.

29. Venue is proper in this District under 28 U.S.C. § 1391 and 15 U.S.C. §§ 15, 22, and 26.

30. Mastercard is found in, transacts business in, and/or has an agent in this District. Mastercard has an office within this District at 225 Franklin Street, 9th Floor, Boston MA 02110. Mastercard describes its Boston office as "a hub of innovation, collaboration …," and it routinely recruits directors and vice presidents to work in this office. Additionally, banks are found in this District which issue Mastercard branded cards to consumers in this District; consumers use

Mastercard branded cards in this District; merchants accept Mastercard branded cards in this District; and banks acquire Mastercard branded card transactions in this District, all in-District activities facilitated by Mastercard. Mastercard provides credit and debit card payment systems and/or services in this District, including for consumer-merchant mobile wallet contactless payment transactions. Mastercard's anticompetitive conduct involves interstate commerce and a United States-wide market, with the acts complained of having a substantial anticompetitive effect in this District and with the impacted interstate commerce affected by Mastercard's antitrust violations being carried out in part in this District.

31. Furthermore, OV Loop's principal place of business is in this District and has been since its inception over six years ago. OV Loop is currently headquartered in Woburn, Massachusetts. OV Loop's physical office is in this District. Most of OV Loop's domestic employees are in this District, including its senior management (C.E.O, Senior Vice President, and Chief of Staff, along with its finance and HR department, and its software development and quality assurance team members).

IV. STATEMENT OF FACTS: CARD NETWORKS, MOBILE WALLETS, AND SUPER-APPS.

32. Over the past decades, payment cards have transitioned through four distinct epochs: (1) plastic cards with static magnetic stripe data; (2) chip-enabled cards with some dynamic data; (3) mobile wallets with more dynamic data; and (4) payment super-apps, which bypass the card networks, cost pennies on the dollar, are more fraud-resistant, and let the purchaser control the purchaser's data. Given the actions of Mastercard, American consumers are trapped in the third epoch — mobile wallets — and have no access to a super-app. This is bad for consumers and inimical to the very process of competition.

A. The Old Plastic Economy: Card Networks, Banks, and Processing Fees.

33. Banks issue both credit and debit cards, with credit cards being the most popular form of payment worldwide. Initially, credit and debit cards were made of plastic with hard-coded and embedded account data on a magnetic stripe. This "static data" included the funding PAN, expiration date, and the card verification value ("CVV"). These card's magnetic stripes could be swiped at readers at physical stores, or the payment information embossed or displayed could be entered into online forms or read to a merchant over the phone. Banks charge fees (set by the card networks) for the use of such cards in stores, online, and over the phone and may collect interest on carried balances.

34. Then and now, almost all banks use either Mastercard or Visa as the "network" to process non-check consumer-merchant payment transactions.

35. "Payment rails" are the infrastructure that facilitates the transfer of funds between parties, such as individuals, businesses, and financial institutions. Payment rails are networks that make it possible to process payments, including credit and debit card payments. They transmit information during a transaction, such as an account number or merchant identification number, between the payer and payee, no matter their location or preferred currency. The card networks, *e.g.*, Mastercard, provide the payment rails that credit and debit transactions use. An example of a non-card payment rail is ACH transactions, operated by the National Automated Clearing House Association, which is used by peer-to-peer ("P2P") payment applications, such as PayPal, Venmo, and Zelle. P2P applications facilitate consumer-to-consumer payments, as opposed to consumer-to-merchant payments. It is consumer-to-merchant payments, not consumer-to-consumer payments, that are the bread and butter of the card networks' business, including Mastercard, due to their ability to collect a fee on every transaction.

36. When accepting payment through a Mastercard branded card, the merchant perforce pays a "merchant discount fee" which includes an "interchange fee," typically set as a percentage of the transaction value. These interchange fees, while collected by the banks, are set by Mastercard and Visa, and a portion of these collected fees are rendered to Mastercard.

37. Issuing banks compete for customers by offering various card products, including credit cards, debit cards, store value cards, and other prepaid products which may or may not carry additional features such as the ability to earn "cash back" or loyalty incentives, and the like.

38. Mastercard and Visa have long been the subject of legal proceedings on antitrust grounds. The two companies set the interchange fee. Each maintains a relationship with member banks and maintains agreements tying these individual banks to Mastercard and Visa processing networks. Practices employed by Mastercard and Visa have been found unlawful under the antitrust laws. *See, e.g., generally United States v. Visa U.S.A., Inc.*, 344 F.3d 229 (2nd Cir. 2003). As of July 2023, Mastercard and Visa are facing a new antitrust lawsuit that alleges they conspired to vastly overcharge Block (the Square payment platform), causing higher retail prices to be paid by consumers. *See Block, Inc. v. Visa, Inc.*, No. 23-cv-05377-MKB-VMS, at Dkt. No. 1 (E.D.N.Y) (case initiated Jul. 14, 2023).

39. Mastercard has been adjudicated to possess market power independent of Visa. *See, e.g., United States v. Visa U.S.A., Inc.*, 344 F.3d 229, 239 (2nd Cir. 2003) ("We agree with the district court's finding that Visa U.S.A. and MasterCard, jointly and separately, have power within the market for network services"). Mastercard has the ability to exclude competition and control prices. It can set the terms of its relationships with merchants (with an ultimate impact on the consumer). This includes setting the fees it charges for processing transactions and tying banks to its network. The reason behind Mastercard's dominance is its historical and ongoing use of

anticompetitive strategies to benefit itself, foregoing short-term profits for longer-term anticompetitive gain. As a result, Mastercard sets supracompetitive processing fees and reaps supracompetitive profits from those fees.

B. Epoch Two: Chip Enabled Smartcards.

Cryptograms

40. Most credit/debit card fraud does not come from people stealing and using cards. Rather, it comes from people stealing card data: the original PAN; the expiration date; and the CVV. With this data, thieves ("fraudsters") can then purchase items online or quickly clone a physical card.

41. This is all possible because traditional card data is static: it does not change transaction-by-transaction; it does not change over time (except over years). Making payment data "dynamic," so that the data changes with every transaction, or in short-preset intervals, has been a pivotal financial technology ("FinTech") goal for decades. Stealing one-time payment data yields little to criminals.

42. Early attempts focused on making magnetic stripe data dynamic in order to increase payment security without having to replace merchant point-of-sale (POS) terminals. However, building a card that can change magnetic stripe data on the fly, as swiped, presents a difficult engineering challenge. POS terminals had very tight swipe time and data communication requirements, and the early dynamic magnetic stripe cards would often not satisfy these hurdles. A debit or credit card that works only some of the time is not a marketable product.

43. Another attempt involved using cards with integrated circuit cards ("ICC"), that is plastic payment cards equipped with an onboard CPU and tamper-resistant memory, together called a Secure Element ("SE"). The SE could generate dynamic payment data in the form of a

type of encrypted data known as a "cryptogram" when inserted into a POS reader. These chip-based cards, however, required new POS terminals that could read the chip (in addition to traditional magnetic stripes). Put differently, successful deployment of this technology required not just the issuance of new cards to millions of Americans, but the installation of new card readers at merchants across the country. After many years, the transition was made to chip-based payment cards, "smartcards."

44. A smartcard's SE is used to securely store a permanent cryptographic key (a type of key used for encrypting data) and an original/funding PAN (which was also embedded in the Track 1 and Track 2 data of the card's magnetic strip and printed onto the card's physical surface). The SE also contains a secure applet approved by EMVCo that allows interaction with a compatible EMVCo smartcard-enabled POS reader during a transaction via the International Organization for Standards ("ISO") 7816 communication protocol.

45. The "EMV" in EMVCo stands for Europay Mastercard Visa. As its name suggests, EMVCo is a payment card network consortium. It sets standards that must be followed with respect to smartcard (and mobile wallet) credit and debit card transactions, which, per these standards, must use the security feature known as a cryptogram. EMVCo first promulgated standards for smartcards in 1993. Per EMVCo's specifications, a smartcard generates dynamic cryptograms for use in authorizing transactions attempted with the smartcard. EMVCo is overseen by its six members: the four United States card networks, *i.e.*, Mastercard, Visa, American Express, and Discover; the Japanese card network, JCB; and the Chinese card network, UnionPay.[2] The card networks' control over this standard-setting body is accomplished through EMVCo's Board of Managers, which consists of two representatives from each member network, and the EMVCo

[2] Europay was acquired by Mastercard.

Executive Committee, which consists of member network representatives. Mastercard's current EMVCo Board representatives hold Vice President titles at Mastercard.

46. At the time of producing an EMVCo-compliant smartcard, the permanent cryptographic key and funding PAN, along with other Track 1 and 2 data, are provisioned to the card's SE, and the card is then mailed to the consumer, who can then insert the card into EMVCo smartcard enabled POS readers to make a payment. At the time of a transaction, the smartcard generates dynamic cryptograms (encrypted data) that can be verified by the payment network's backend system. Smartcards were engineered to change payment data, transaction-by-transaction, or over short time periods; the dynamic cryptogram used yesterday would not work today.

Tap-to-Pay: NFC

47. Smartcards were originally insertion only, *i.e.*, their chip needed to be inserted into a chip-card reader in order to be read. Later, smartcards were made to work with not just contact readers using the ISO 7816 protocol, but also with contactless readers using the ISO 14443 protocol to enable tap-to-pay. With tap-to-pay, one could just tap a contactless-enabled chip-card against a "contactless" near field communication ("NFC") enabled POS reader to initiate a contactless transaction. NFC is a short-distance radio transmission. In these contactless smartcards, transactions are facilitated by a permanent cryptographic key, a funding PAN, and the network-approved payment applet, all stored on the card SE.

48. These contactless-enabled smartcards required upgraded, *i.e.*, NFC enabled, readers at merchants. Until several years ago, these contactless tap-to-pay products were not accepted in most merchant locations (fewer than a third of the POS terminals in the United States were NFC-enabled prior to 2011). This has changed over the past decade with tap-to-pay, or "contactless" payments, rapidly increasing in popularity.

Fraud Continues

49. Smartcards have not eliminated fraud. For example, a major security weakness with smartcards comes with "card not present" transactions (*e.g.*, buying a product online). In these cases, smartcards are no smarter than their static magnetic stripe counterparts. The percentage of "card not present" transactions is growing rapidly.

50. With smartcards, Mastercard continues to set supracompetitive processing fees and reap supracompetitive profits from those fees.

C. Epoch Three: Mobile Wallets.

Digital Wallets and Tokenization

51. There are two basic types of retail commerce today—online (or "e-commerce") and in-store (or traditional "brick-and-mortar stores" ("B&M"), *e.g.*, the neighborhood CVS). Combined United States e-commerce and B&M sales for 2022 totaled more than $5 Trillion. Today, in the United States, approximately 85% of all retail transactions take place in B&M retail locations, while circa 15% of such transactions occur online. The online commerce retail percentage is growing rapidly, however, year-over-year.

52. A digital wallet application is an application on a mobile device, desktop, or on the Web loaded with payment information, *e.g.*, credit and debit cards. For example, the Apple Pay application, loaded on the iPhone, is a digital wallet application, as is a Samsung Pay/Samsung Wallet application loaded on a Samsung phone. The wallet application need not be hosted on a phone, but can instead reside on a key fob, or an electronic watch, or any other small, electronic device, *e.g.*, a Garmin smartwatch. Digital wallet functionality can also be used for online shopping from a web browser, including on a desktop. In instances where the digital wallet application resides on a mobile device and can at least be used for B&M purchases, it is a mobile

wallet. Where the digital wallet is exclusively for e-commerce transactions, it is an e-commerce wallet. In addition to being able to be used at B&M locations, a mobile wallet may also support e-commerce payments. Apple Pay is such a mobile wallet: you can use it to tap-to-pay at your local coffee store, and while waiting on your coffee, use it to pay for an online purchase.

53. Digital wallets use virtual credit/debit cards, which typically have a real-world plastic counterpart. One obvious advantage to a digital wallet is that it collects all card and payment information in one place (so, for example, to complete an online purchase, you just need to pick which virtual card you want to use; you do not have to enter payment information into an online form). But that is not the principal benefit of a digital wallet. Through the evolution of digital wallets, a new security paradigm emerged: tokenization. As now mandated by card network standards, mobile wallets **must** communicate with retailers using not only dynamic cryptograms but also obfuscated conventional card data account identifying information that can change over the life of the card, *i.e.*, mobile wallets must use (and e-commerce wallets may use) tokenization.

54. Mastercard and Visa transitioned to e-commerce in the 1990s and later fully embraced digital payments to support their payment network methods on desktops and mobile devices, including via the likes of Apple Pay and Samsung Pay.

55. Digital payments are important to commerce in the United States and will continue to become increasingly important in the years to come. That is, consumers will use their phones, smartwatches, or other digital devices to purchase goods, both online and in retail, B&M locations. Both Mastercard and Visa view this digital payment business as existentially important

to their brands, business, future, and cash flow.[3]

56. Mastercard and Visa have, over the past several years, made a concerted push into the digital payments arena. For example, both companies implemented their own e-commerce wallet solutions with Masterpass by Mastercard and Visa Checkout by Visa. These solutions were then replaced with Mastercard Click to Pay and Visa Click to Pay, which are based on a card consortium (EMVCo) standard. These e-commerce card network wallets work with the card networks' tokenization services. And, unlike smartcards, e-commerce wallets and mobile wallets with e-commerce functionality can use cryptograms to secure online payments.

57. Mastercard and Visa also provide tokens to mobile wallets; in fact, they mandate that mobile payments use tokens. *See* below. Both Mastercard and Visa act as TSPs for their branded cards, *i.e.*, they obfuscate (tokenize) for card issuers a consumer's funding PAN by replacing it with a tokenized PAN, maintain a mapping of the funding PAN to the tokenized PAN, and restore (detokenize) the tokenized PAN to the original PAN.

58. For example, if a consumer wishes to load his or her mobile wallet with a Mastercard branded card, he or she enrolls it by entering its funding PAN into the mobile wallet application. The wallet application does not store the original PAN—it is the funding PAN that serves to directly identify the consumer's account with the bank issuer. Instead, the wallet's

[3] *See, e.g.*, Mastercard, Inc., Form 10-K for Fiscal Year ended Dec. 31, 2022 at 8, available at https://d18rn0p25nwr6d.cloudfront.net/CIK-0001141391/3f400cd7-b9fb-4732-9e59-c669ea4fe0cc.pdf ("Our Key Strategic Priorities[:] Expand in payments … We do so by: Driving growth in consumer payments with a focus on accelerating digitization[.]"); Visa Inc., Form 10-K for Fiscal Year ended Sep. 30, 2022 at 4, available at https://www.sec.gov/Archives/edgar/data/1403161/000140316122000081/v-20220930.htm ("OVERVIEW[:] Visa is one of the world's leaders in digital payments …. We are accelerating the migration to digital payments [.]"); *Id*. at 8 ("The provisioning of network tokens continues to accelerate. As of the end of fiscal year 2022, Visa provisioned more than 4 billion network tokens, surpassing the number of physical cards in circulation. The milestone reinforces Visa's commitment to secure, seamless, digital payments, in-store and online").

backend submits it to Mastercard and requests from Mastercard a token (a tokenized PAN), which will be stored in the mobile wallet and used in payment transactions in the funding PAN's stead. The mobile wallet provider is a TR, while Mastercard is the TSP. The wallet application's stored token is not static; this token can be swapped out for a new token over the life of the corresponding original PAN. For example, the TR (mobile wallet provider) may request a new token from the TSP (Mastercard) after the old token is used for a preset number of transactions.

59. As explained above, making the payment card information that is passed onto merchants' dynamic increases card security; this is especially true for account identifying information. Token use has other benefits too. For example, if the consumer loses his or her mobile device, just the token registered to the mobile wallet on the device needs to be canceled—the user need not replace his or her physical card, as the funding PAN on that card was not exposed by the loss of the device.

60. Both Mastercard and Visa control and dominate the tokenization services that issuers use to obfuscate funding PANs. Through its size, strength, and structural advantages, along with efforts to exclude competitors, Mastercard made other 'would be' TSPs for Mastercard branded cards uncompetitive. For example, at least initially, the relevant EMVCo specifications mandated that only card networks could be TSPs. *See* Pandy & M. Crowe, *Understanding the Role of Host Card Emulation in Mobile Wallets, Payment Strategies,* Federal Reserve Bank of Boston (May 10, 2016), available at https://www.bostonfed.org/publications/payment-strategies/understanding-the-role-of-host-card-emulation-in-mobile-wallets.aspx ("For now, only card networks can serve as TSPs but the specification is being updated to include requirements for non-network TSPs"). Not even the card issuers (*e.g.*, banks) could compete with Mastercard and Visa. Today, if an issuer needs token services for a branded credit or debit card,

it uses that brand's tokenization service.[4] This, in turn, has made Mastercard the gatekeeper to mobile wallet compatibility with consumer's Mastercard cards. Accordingly, if a mobile wallet provider wants its mobile wallet to work with a bank's Mastercard branded card, it **must** have access to the tokens Mastercard generates for the bank. In short, Mastercard controls the distribution of tokens for thousands of banks to mobile wallets such as Apple Pay, Samsung Wallet, and Google Pay, and thus controls the viability of a given mobile wallet.

61. At least initially, Mastercard charges issuers and acquirers "digital enablement fees" for its mobile wallet tokenization services, including charges of 50 cents per token provisioned and 10 cents per token per month maintained on a mobile wallet. *See* As Card-Industry Use of Tokens Increases, MasterCard Plans "Digital Enablement" Fees, Aug. 14, 2014, available at https://www.digitaltransactions.net/As-Card-Industry-Use-of-Tokens-Increases-MasterCard-Plans-Digital-Enablement-Fees-/ ("MasterCard Inc. is planning new 'digital enablement' fees, one for merchant acquirers and the other for card issuers, that will generate revenue for the network as mobile payments and the use of tokens that substitute for actual payment card numbers increase . . . . They include a 'Digital Enablement Service Lifecycle Management' fee of 10 cents per PAN, billed monthly. MasterCard also will charge a 50-cent 'digitization' fee each time a mobile device is provisioned with a token, and 2.5 cents for calls to its 'alternate network application programming interface."'). The digital enablement fees described above are distinct and in addition to Mastercard's traditional, supracompetitive interchange fees.

62. Mastercard has already been sanctioned by the Federal Trade Commission for engaging in illegal anticompetitive conduct through its use of its TSP for debit card transactions.

[4] Even American Express and Discover are non-competitive; relegated to performing token services for the cards they issue themselves as banks.

See FTC Orders an End to Illegal Mastercard Business Tactics and Requires it to Stop Blocking Competing Debit Card Payment Networks, December 23, 2022 (FTC order ending the "illegal business tactics that Mastercard has been using to force merchants to route debit card payments through its payment network . . . . Specifically, Mastercard used its control over a process called 'tokenization' to block the use of competing payment card networks [by] . . . refus[ing] to provide [token] conversion services to competing networks for remote ewallet debit transactions (*i.e.*, online and in-app transactions, as opposed to in-person transactions made by the customer in a store), thereby making it impossible for merchants to route their ewallet transactions on a network other than Mastercard."), available at https://www.ftc.gov/news-events/news/press-releases/2022/12/ftc-orders-end-illegal-mastercard-business-tactics-requires-it-stop-blocking-competing-debit-card.

MST

63. Mobile devices with mobile wallets, like their contactless smartcard predecessors, use NFC to communicate with B&M POS terminals. Despite significant effort, however, United States NCF terminal penetration stands at 70 percent. Many smaller merchants, including restaurants and stores with older terminals, have not upgraded, and even some large retailers, *e.g.*, Walmart, do not accept NFC payments. Some mobile wallets were able to close this gap in contactless acceptance by taking advantage of a technology called Magnetic Secured Transmission ("MST") which resides on the mobile device.

64. With MST, dynamic payment data can be generated and transmitted to virtually any POS terminal through its traditional magnetic stripe reader, regardless of whether the terminal has been insert-chip or NFC enabled. Hardware on an MST-equipped device emulates magnetic card swipe data so that the payment device can be read by virtually any POS terminal. The

hardware does so by sending current through embedded wire coils that generate pulses of magnetic fields that mimic (emulate) the swipe data, and communicate the data to the POS terminal, without using NFC. MST, thus, makes contactless mobile payments work with well over 90 percent of legacy POS terminals in the country.

65. MST was developed by LoopPay. In 2012, payment POS pioneers George Wallner and Will Graylin began working on this new tap-to-pay communication method. Three years later, in 2015, Messrs. Graylin and Wallner sold their company, LoopPay, to Samsung for roughly $320 million, including post-close earnouts. It became part of Samsung Pay, where Mr. Graylin was the Global Co-GM. In that role, Mr. Graylin helped launch Samsung Pay with the MST technology built into hundreds of millions of Galaxy phones starting in 2015, including Galaxy smartwatches. As Global Co-GM, Mr. Graylin worked directly with the card networks, including Mastercard, on Samsung Pay network certification. Mr. Graylin has since left Samsung and is now OV Loop's C.E.O.

Mobile Wallets on Traditional SE Mobile Devices

66. Just as mobile wallets were initially built on smart cards' use of NFC, they also built on smart cards' use of secure elements. Indeed, the earlier mobile wallets did not have the tokenization advantages they have today over smart cards; they were basically another smart card in a different form.

67. Circa 2010-2013, a mobile wallet running on Visa or Mastercard's rails used a type of cryptographic key, a permanent cryptographic key, that was loaded onto a mobile device's secure element. Mobile device SE stored permanent cryptographic keys are unchanging (or static) throughout the life of a card, secure element, mobile device, or digital credential. When these mobile wallets were used for a B&M contactless transaction, the permanent cryptographic key was

used to generate a cryptogram that was passed along to the POS terminal, and onto the card network for use in an authorization decision. In these systems, the very same device SE stored cryptographic key would be used to generate the cryptogram in every transaction over the life of the card.

68. In these circa 2010-2013 systems, dynamic payment data was limited to the generation of cryptograms using pre-installed permanent cryptographic keys. There was no obfuscated original payment card number—no tokenized PAN—for example.

69. In these devices, the SE performed two functions: (1) secure storage of the permanent cryptographic key and other card data (*e.g.*, the funding PAN); and (2) execute EMVCo-compliant applets to perform the responses needed to communicate with the contactless reader to perform transactions. At the time, the broader industry assumed that an SE was required to achieve secure contactless payments on a smartphone. This was because storing the permanent cryptographic key and funding PAN outside the SE risked them being compromised, *e.g.*, stolen by malicious software on the phone's general operating system. If a smartphone's permanent cryptographic key and funding PAN were compromised, it could result in multiple fraudulent transactions, which could be repeated across POS systems. Not using an SE would significantly increase the issuing banks' risk exposure. Thus, the use of an SE to store the permanent cryptographic key was the industry prescribed standard.

70. Mobile device permanent cryptographic keys and funding PAN provisioning was done by an entity called the Trusted Service Manager ("TSM") over the air. The mobile device SE had to be securely provisioned and had only one point of access with one key. This process was typically controlled by the Mobile Network Operator ("MNO"), regardless of whether the MNO also served as the TSM. Whoever controlled SE access controlled what mobile wallet

applications could be on a given mobile device.

71. The use of device SEs loaded with permanent cryptographic keys resulted in a lot of complexity, as each issuer needed to have a relationship with the TSM and/or MNO to facilitate the provisioning process, and many smartphones did not support SEs. While many mobile device makers installed NFC capabilities on their smartphones, most did not install SEs due to the extra cost. Mobile wallet provider reliance on device SE stored permanent cryptographic keys was a particularly complex and costly endeavor, as it required the cooperation of handset manufacturers and/or mobile network operators.

72. Unsurprisingly, this resulted in a lack of interest in mobile wallets. This lack of interest was due to the fragmented device technology: some mobile devices had SEs, and some did not; MNO fragmentation: some MNOs supported SE for mobile wallets while others did not; issuer fragmentation: some banks supported a MNO's SE mobile support while others did not; and merchant fragmentation: some merchants supported contactless POS readers while others did not. All of this resulted in an unsatisfactory mobile payment environment.

73. In short, using device SEs loaded with permanent cryptographic keys hindered mass deployment of secure mobile payment systems (and with it the arrival of tokenization). *See* J. Heggestuen, *What the Newest Mobile Payments Tech, 'Host Card Emulation,' Means for the Industry*, INSIDER (Jul. 30, 2014), available at https://www.businessinsider.com/host-card-emulation-doesnt-overcome-most-important-problem-in-payments-2014-7 ("Until now, the problem with an NFC-based system is that there is one party — usually the carrier — that acts as a gatekeeper for who and what can access the secure element. If a company wanted to build a mobile payment app that uses NFC-based payments, it would need to partner with the gatekeeper and rent space on the secure element. This is further complicated by the fact that storage space on

the secure element is limited, which means having a handful of mobile wallets on a mobile phone won't work. Beyond the complexity and cost of establishing a relationship with a third party, some mobile carriers have a vested interest in limiting access to the secure element because they offer their own mobile wallets").

HCE Mobile Wallets

74. In 2014, with support from Mastercard and Visa, Google moved away from mobile device SE-stored permanent cryptographic keys with the announcement of a cloud-based system for contactless mobile wallet payments on Android devices. This system did **not** require that the mobile device contain an SE loaded with a permanent cryptographic key, be it a smartphone, which Google was not the manufacturer of most of the time, a fob, or a smartwatch, etc. Instead, the cloud would provide or emulate a SE, using solutions such as Hardware Security Modules, to generate "non-permanent cryptographic keys" that could be sent to mobile devices and stored in the devices' memory along with an account identifier (*e.g.*, a tokenized PAN). These cloud-derived non-permanent cryptographic keys do not have to be stored in a tamper-resistant chip, such as a device SE, even though they could be, because these keys, which are also used to generate one-time-use cryptograms, can change, thus limiting the key's usefulness if stolen by other code running in the general operating system of the mobile device.[5]

75. In this cloud-based solution, using a non-permanent cryptographic key, the mobile device can generate and send to a POS terminal a one-time-use cryptogram and, for example, a tokenized PAN (but not the non-permanent cryptographic key). Then, with the tokenized PAN in hand, the remote cloud system can identify the non-permanent cryptographic key that should have been used to generate the response cryptogram and generate its own cryptogram. If the cloud

[5] A tokenized PAN also does not have to be, but could be, stored in an SE; with a tokenized PAN, the funding PAN is masked.

system-generated cryptogram and the mobile device cryptogram do not match, then the transaction will not be authorized. The cloud system can also detokenize the PAN so that the original PAN can be sent to the issuer, allowing the issuer to verify that there are sufficient funds for the transaction.

76. Google announced cloud-derived non-permanent cryptographic keys as an innovative and novel advance in payment technology and security. Since 2014, mobile wallets for Android phones (including Samsung Pay/Wallet) have used cloud derived non-permanent cryptographic keys.

77. This cloud-based non-permanent cryptographic key generation method and system was developed by SimplyTapp, a now wholly owned OV Loop subsidiary. SimplyTapp coined the phrase "Host Card Emulation," or "HCE," to refer to the cloud-based mobile payment technology it developed that eliminates reliance on device SEs, including the form of HCE that uses non-permanent cryptographic keys.[6] HCE is the term used throughout the industry today, and SimplyTapp is widely credited as the originator of HCE. *See, e.g.*, J. Heggestuen, *What the Newest Mobile Payments Tech, 'Host Card Emulation,' Means for the Industry*, INSIDER (Jul.

[6] SimplyTapp's founder, Doug Yeager, is the sole inventor on OV Loop's United States Patent No. 10,032,171, "Systems and Methods for Secure Application-Based Participation in an Interrogation by Mobile Device" (the "'171 Patent"). Loosely speaking, the '171 Patent claims storing remote computer system derived non-permanent cryptographic keys on a mobile device for generating, by a mobile payment application, cryptograms for use in facilitating in-store purchases. The '171 Patent's claims are agnostic as to where non-permanent cryptographic keys are stored or are capable of being stored on a mobile device. The non-permanent cryptographic keys could be stored in a mobile device Rich OS, trusted execution environment, or SE, for example.

OV Loop filed suit against Mastercard for infringement of the '171 Patent. That action: *OV Loop, Inc. v. Mastercard Incorporated*, No. 7:23-cv-1773-CS (S.D.N.Y.), is stayed pending resolution of two *inter partes* review petitions challenging the '171 Patent: *Mastercard Incorporated v. OV Loop, Inc.*, Nos. IPR2023-01289 & IPR2023-01290 (Patent Trial & Appeal Board), filed by Mastercard.

30, 2014), available at https://www.businessinsider.com/host-card-emulation-doesnt-overcome-most-important-problem-in-payments-2014-7 ("Host card emulation (HCE) is the latest technology driving a new wave of excitement in the mobile payments industry. The new feature, which was first developed by a company called SimplyTapp, was recently deployed by Google with Android 4.4. (KitKat) and quickly received the backing of the major card networks").

78. The significant benefits of HCE have been extolled by the trade. For example, Rambus, "a leader in high-performance memory subsystems, providing … innovations that maximize the performance and security in data-intensive systems," https://www.rambus.com/corporate-overview/, described HCE as follows:

> Placing the payment credentials in a remote environment, communicating via the cloud, rather than in a secure element (SE) inside the mobile device, offers more control and direct access to application issuers and eases the launch and use of NFC based mobile services.
>
> - **The Benefits of HCE…**
>
> - The main advantage of HCE is the ability it has to put service providers in control of costs, security, partners and, most importantly, management of a solution's position in the value chain. Players in the NFC ecosystem want to work under mutually beneficial and productive relationships, which will ultimately drive the technology forward and add value to the end-user.
>
> - Here are some of the other benefits that HCE offers:
>
> - **Independence**
>
> - By deploying services to devices via HCE, service providers don't need to set up any other commercial relationships. This narrows the gap between application issuers and customers, ensuring a consistent brand and end-user experience across all available NFC services.
>
> - **Easier integration with third parties**
>
> - Easy access to the SE via the cloud allows easy integration with any third-party provider and business model.

- **Lower costs**
    - SE integration in mobile devices can be expensive and subject to SE domain fees. By deploying the SE remotely, the NFC value chain will be shortened as fewer parties in the ecosystem need to be involved, leading to lower provisioning costs.
- **Enhanced security measures & improved risk management**
    - Direct access to the SE enables instant fraud detection and allows immediate blocking of an application. Additionally, the computing power of HCE is higher than that on a mobile device. Enhanced security means better customer satisfaction and higher adoption in the long-term.
- **Multiple cards, EMV applications & payment schemes**
    - Storage capacity on a physical SE is limited. Using HCE, storage is scalable and can be expanded to meet individual requirements and to support any card, application and payment scheme.
- **Compatibility with readers and POS**
    - As the transaction emulates an EMV payment, no changes are needed to existing contactless terminals or the payment acceptance infrastructure.

Host Card Emulation in Android: What does it Mean? (originally posted on Nov. 13, 2013; last updated on Aug. 8, 2016), available at https://www.rambus.com/blogs/host-card-emulation-in-android-what-does-it-mean/; *see, also, e.g., What is Host Card Emulation?* available at https://www.verimatrix.com/knowledge-base/digital-payment/what-is-host-card-emulation/ ("The more recent cloud environment has shown to improve on the complexities of a physical SE solution. The benefits cross both the merchant platform and consumer experiences in terms of HCE mobile payments") (Verimatrix is a digital security company).

79. The benefits of HCE were also recognized by Mastercard and Visa who adopted HCE specifications for HCE mobile wallets. *See, e.g., Mastercard to Use Host Card Emulation*

(HCE) for NFC-Based Mobile Payments, Mastercard Press Release, Feb. 19, 2014 ("Mastercard today announced it will publish a specification that leverages Host Card Emulation (HCE) for secure near field communication (NFC) payment transactions … HCE enables payments … to be delivered without the use a secure element (SE). The specification … marks a significant industry milestone that, in addition to MasterCard's longstanding support for embedded and SIM-based SE implementations, will drive greatly expanded availability of mobile contactless payments for customers"); *Visa to Enable Secure, Cloud-Based Mobile Payments*, Visa Press Release, Feb. 19, 2014, available at https://investor.visa.com/news/news-details/2014/Visa-to-Enable-Secure-Cloud-Based-Mobile-Payments/default.aspx ("Visa's support for cloud-based payments follows the introduction of a new feature in the Android mobile operating system called Host Card Emulation (HCE) …. Standards: Visa has enhanced its contactless payment application, Visa payWave, and is introducing a new standard, requirements, program approval process and implementation guidelines to enable financial institutions to securely host Visa accounts in a virtual cloud …. Services: Visa is developing a new service and platform, to enable clients and partners to issue Visa accounts digitally – in the cloud … linked to a digital wallet. The solution will also enable the issuance of payment tokens that will replace the 16-digit payment account number and can be limited for use with a specific device ….").

80. In fact, both Mastercard and Visa engaged with OV Loop's now subsidiary, SimplyTapp, with respect to the adoption of HCE for mobile payments. *See, e.g.*, *Host Card Emulation Becomes Reality With Card Networks Adoption*, Marketwired (Feb. 20, 2014), available at https://www.yahoo.com/news/host-card-emulation-becomes-reality-130000472.html ("Today is an exciting day for the mobile industry as VISA, Inc. and MasterCard Worldwide, Inc. announced their support of Google's adaptation of the NFC tap and pay Host Card Emulation

(HCE) architecture …. SimplyTapp will continue to work closely with both Visa and MasterCard … to lead the adoption of mobile payment experiences through the use of … HCE …. SimplyTapp will be participating on Visa's HCE panel at this year's Mobile World Congress 2014").

81. The novelty, success, and continued promise of the HCE approach is confirmed by the recognition SimplyTapp received. For example, a September 2012 trade press article described SimplyTapp's HCE as unconventional:

> The concept runs counter to accepted wisdom on how to keep sensitive transaction data secure with a mobile phone. NFC security standards for 'card emulation mode' … are based on the idea that a mobile phone is not a safe environment for sensitive data[;] [a]ll such data, therefore is stored within a physical secure element on the phone ….

S. Clark, *SimplyTapp Proposes Secure Elements in the Cloud*, NFCWORLD (Sep. 19, 2012), available at https://www.nfcw.com/2012/09/19/317966/simplytapp-proposes-secure-elements-in-the-cloud/. Later, a July 2014 Business Insider article described SimplyTapp's HCE as a new technology that generated much excitement in the mobile payment space:

> Host Card Emulation (HCE) is a technology that **breathes new life** into near field communication …. Prior to HCE, mobile wallet providers needed to store payment credentials in a highly restricted part of the smartphone controlled by mobile carriers. HCE gets around that, thus lowering the barrier to entry for NFC mobile wallets …. Host card emulation (HCE) is the latest technology driving a **new wave of excitement** in the mobile payments industry. The new feature, which was first developed by a company called **SimplyTapp**, was recently deployed by Google with Android 4.4 (KitKat) and quickly **received the backing of the major card networks**…. HCE has created renewed momentum for NFC mobile payments by allowing NFC wallet providers to get around the 'secure element,' …. Bypassing the secure element makes it easier for providers to develop mobile NFC wallets.

J. Heggestuen, *What the Newest Mobile Payments Tech, 'Host Card Emulation,' Means for the Industry*, Insider (Jul. 30, 2014), available at https://www.businessinsider.com/host-card-emulation-doesnt-overcome-most-important-problem-in-payments-2014-7. A year later, SimplyTapp was "awarded Best Contactless Payments Solution of the Year at the 2015 Future

Digital Awards." M. Clark, *SimplyTapp Picks Up Contactless Payments Award*, NFC WORLD (Aug. 25, 2015), available at https://www.nfcw.com/2015/08/25/337201/simplytapp-picks-up-contactless-payments-award/. These awards are organized by well-known digital technology research firm, Juniper Research, whose Head of Forecasting and Consultancy said that:

> SimplyTapp's offering essentially redefined and reinvigorated an NFC market that was in danger of stagnation …. Its solution has provided the technological backbone for stripped-down business models that can deliver products to market far more quickly and economically than was previously the case; it has reignited the interest of the financial services sector in the mobile contactless market.

Id. (quoting SimplyTapp press release quoting Juniper Research).

82. To this day, the innovations developed by SimplyTapp continue to drive mobile payment growth. *See Contactless Payment Global Market Report 2022: Adoption of New Technologies Such as Host-Based Card Emulation and NFC Bolsters Sector*, RESEARCH AND MARKETS (Feb. 27, 2023), GlobalNewswire by notified, available at (https://finance.yahoo.com/news/contactless-payment-global-market-report-124800418.html?fr=sycsrp_catchall) ("Growing adoption of new payment technologies, such as Host-based Card Emulation (HCE) and Near Field Communication (NFC) for the contactless payments, is anticipated to drive the market growth …. Thales Group, in a survey, stated that by 2023, there would be more than 2.6 billion contactless payment cards in circulation, owing to the technology's rapid adoption in the markets such as … the United States ….").

83. It is HCE that led to the third epoch, the mobile wallet era, by "redefin[ing] and reinvigorat[ing]" mobile payment technology. *See Visa Partners with Financial Institutions Across the Globe to Enable Mobile Payment Services*, Visa Press Release, Feb. 26, 2015, available at https://investor.visa.com/news/news-details/2015/Visa-Partners-with-Financial-Institutions-Across-the-Globe-to-Enable-Mobile-Payment-Services/default.aspx ("'Host Card Emulation has

opened up the Android payments ecosystem to innovation, democratizing access to NFC and paving the way for more rapid uptake of mobile commerce services,' according to Jordan McKee, senior analyst at 451 Research. 'Inevitably, the technology will play a marquee role in driving the proliferation of in-store mobile payments, an opportunity 451 Research projects will reach $570.1 billion globally by 2018.'").

84. HCE led to the proliferation of mobile wallets we see today. HCE also led to mobile wallet tokenization. HCE rendered MNOs (and their TSMs) irrelevant in the mobile wallet space. With the mobile network operators, *e.g.*, Verizon and AT&T, out of the picture, HCE wallets, and even a wallet that remained reliant on stored permanent cryptographic keys, could be readily supplied with tokens.

85. As explained above, Mastercard and Visa are the United States' TSPs. As TSPs, they provide the non-permanent cryptographic keys, in addition to the tokens for their cards, and perform the backend cryptogram check and detokenization for authorization decisions. Mastercard exclusively controls access to its TSP systems and services. There is no government regulator overseeing mobile wallet access to this Mastercard-controlled critical mobile payment infrastructure. Simple economics would dictate that Mastercard would approve as many legitimate mobile wallet providers as possible: more Mastercard certified mobile wallets on consumers' smartphones translates to increased Mastercard token and rail use, which means more interchange fees, i.e., more money, for Mastercard. But, as is the case with OV Loop, Mastercard does not provide this access where it has an anticompetitive incentive not to.

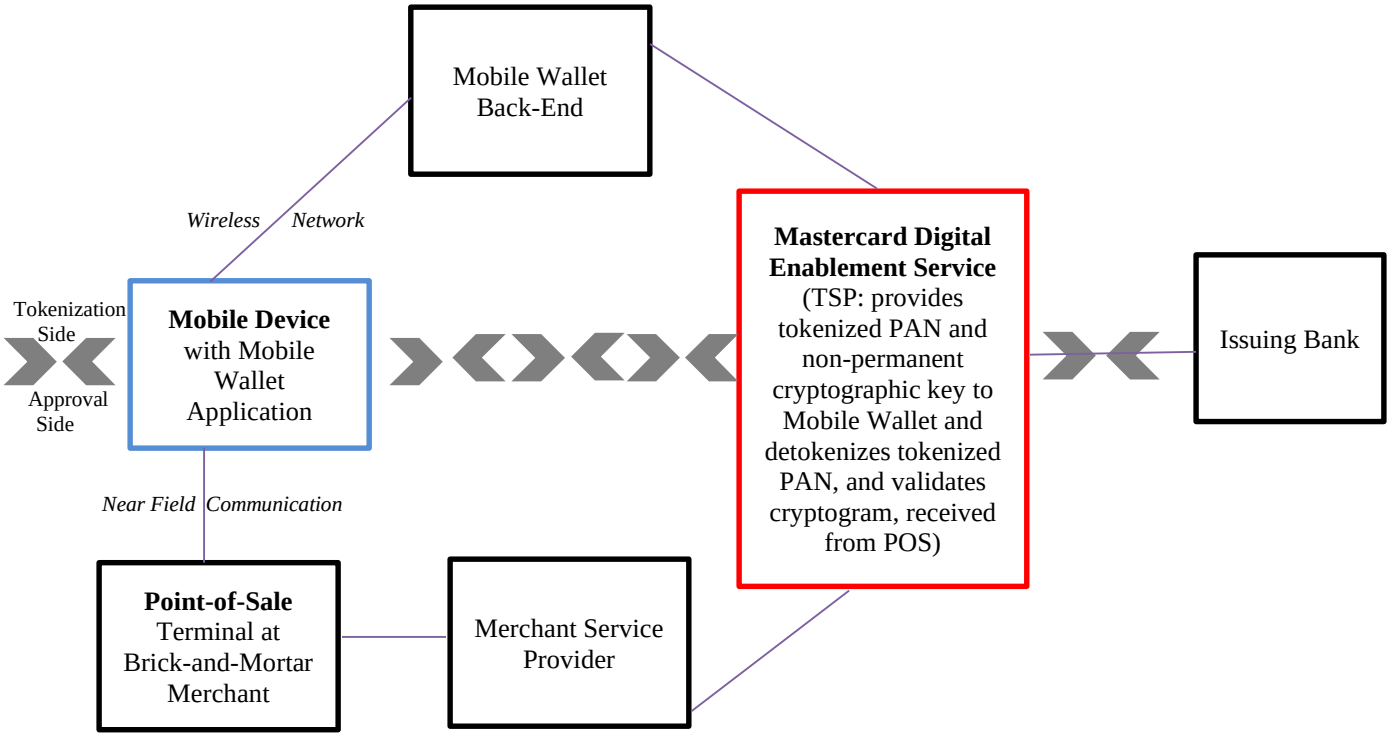
Mastercard's Mobile Wallet Specifications and TSP System

86. Mastercard and Visa promulgate specifications that mobile wallets using their branded cards must meet. For example, Mastercard has a set of standards it calls "Mastercard

Cloud-Based Payments" or "MCBP," which imposes requirements on HCE mobile wallets. Mastercard's specifications governing mobile wallet payments require the use of tokenization, which was standardized by the credit card consortium, EMVCo. *See* Pandy & M. Crowe, *Understanding the Role of Host Card Emulation in Mobile Wallets, Payment Strategies*, Federal Reserve Bank of Boston (May 10, 2016), available at https://www.bostonfed.org/publications/payment-strategies/understanding-the-role-of-host-card-emulation-in-mobile-wallets.aspx ("Following the EMV spec, when a payment card is provisioned to a mobile wallet, the token service provider (TSP) tokenizes the PAN and stores the token … in the phone. Additionally, MasterCard and Visa modified their contactless specifications to support single/limited use keys and cloud cryptograms that recognize HCE tokens as valid payment credentials.").

87. To access Mastercard tokens, a mobile wallet must be certified and licensed by Mastercard. So, for example, if a mobile wallet provider desires to use an HCE solution for its wallet it must get its solution approved by Mastercard in order to connect to Mastercard's tokenization system, MDES. *See, e.g.*, https://developer.mastercard.com/mdes-pre-digitization/documentation/ ("The Mastercard Digital Enablement Service (MDES) is a suite of on-behalf-of (OBO) services that supports the management and generation of digital payment tokens to enable simpler and secure digital payment experiences. MDES was developed to facilitate the transition from consumer account credentials (PAN) to digital credentials (tokens). These digital credentials may be provisioned to mobile devices, enabling consumers to perform payments via existing contactless point-of-sale (POS) systems, or via remote payment use cases such as in-app payments stored on file by merchants and digital Wallet Providers (WP), allowing them to exchange payment cards on file with digital payment tokens.").

88. MDES' placement within an exemplary Mastercard HCE ecosystem is illustrated below:



89. MDES is Mastercard's TSP for tokenization services regardless of whether a connecting mobile wallet uses an HCE solution or some other solution. No matter the method employed by a mobile wallet provider, if it wants access to Mastercard's tokens for the thousands of United States financial institutions that rely on Mastercard's tokenization services, it must first be granted access to MDES by Mastercard. Mastercard has wrongfully refused OV Loop access to MDES because it fears that doing so will usher in a new age of consumer-merchant choice—the age of the super-app.

D. Epoch Four: Super-Apps.

Super-Apps

90. A super-app is a mobile payment and messaging platform that enables the user to

manage many tasks digitally with personalized services, and which fosters direct connections between consumers and merchants. It is one application that helps reduce commerce "friction" (*e.g.*, improving convenience, security, and reducing cost) while improving the relationships between buyers and sellers. These apps typically cover payments, store identity, and enable merchant rewards and engagement across devices and channels. As Professor Scott Galloway of New York University said in his November 2021 New York Magazine article, *Super-Apps Are Inevitable Get Ready for the First $10 Trillion Tech Company*:

> A super-app is a single mobile app that offers basic services including chat and payments, along with a suite of 'mini-apps' from third parties, ranging from stores and restaurants to government agencies. Westerners aren't familiar with them, but across much of Asia, super-apps *are* the internet …. An app reaches *super* status when it knits together a critical mass of services and makes them addictively easy to toggle among, even if they aren't as good as sole-purpose apps. The more services, the stickier and more lucrative.

https://nymag.com/intelligencer/2021/11/facebook-metaverse-super-apps.html (emphasis in original).

91. The ability to facilitate digital payments is essential to widespread adoption of super-apps, which include features like mobile wallets for consumer-merchant B&M and online store transactions, bill pay, and consumer-to-consumer payments. Of these payment features, it is the mobile wallet feature, the feature that facilitates everyday commerce, that is the most critical. As Professor Galloway put it in his article:

> Here is the really mind-bending potential of super-apps: Subscriptions and ads are only part of the full super-app monetization model and not even the most profitable. Taking a direct piece of transactions is staggeringly lucrative, and a company built around payments could make the Facebook and Google of today look small.
>
> **Payment processing is the nonnegotiable super-app service.** It's the glue that integrates core features with those provided by third parties on the platform, and it gives users the simple convenience of not having to enter credit-card information across dozens of apps and websites.

Id., *see also Western Super-Apps Forecasting Disruption from a Super Trend*, Deloitte (2022), at 1, available at https://www2.deloitte.com/us/en/pages/financial-services/articles/super-apps-in-the-us.html ("Integrating a payments platform across services has proven highly profitable for super-apps so far—it will likely be the first place we see super-apps take root in the West").

92. Super-apps offer consumers a simple, one-stop way to manage their digital and daily lives. As a KPMG article explained:

> Super apps essentially serve as a single portal to a wide range of virtual products and services. The most sophisticated — apps like WeChat and Alipay in China — bundle together online messaging (similar to WhatsApp), social media (similar to Facebook), marketplaces (like eBay) and services (like Uber). One app, one sign-in, one user experience — for virtually any product or service a customer may want or need.
>
> Due in large part to their versatility, super apps have quickly become ingrained into users' daily lives. It is not unusual for a WeChat user in China to set up a date with a friend via instant messaging, make dinner reservations, book movie tickets, order a taxi and pay for every transaction along the way, all using one single app.

Huang & M. Siegel, *Super App or Super Disruption? Reshaping the Banking Experience*, KPMG (Jun. 2019), available at https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2019/06/super-app-or-super-disruption.pdf; *see also Western Super-Apps Forecasting Disruption from a Super Trend*, Deloitte (2022), at 2, available at https://www2.deloitte.com/us/en/pages/financial-services/articles/super-apps-in-the-us.html ("No more memorizing a go-to credit card number, since your car insurance purchase can use the same e-wallet as your stock trading account. Better yet, the loyalty benefits accrued while ordering pizza can be applied to paying your phone bill. As more transactions become digitized, collecting new functionality into a single app can ameliorate the inconvenience and inertia customers experience when juggling a dozen different apps").

Super-Apps Abroad

93. Super-apps have been very successful abroad.

94. For example, China has the largest digital buyer population in the world, amounting to more than 780 million people. The most prevalent super-app in the country is WeChat, which facilitates every type of commerce transaction and interaction ranging from large global enterprises to the smallest street vendor. Similarly, Alipay claims to operate with over 65 financial institutions, including MasterCard and Visa, to provide payment services for Taobao and Tmall, as well as over 460,000 online and local Chinese businesses. Tech giant Alibaba's Alipay's payment service alone reaches 678.5 million active users.

95. Super-apps have also enjoyed major success throughout much of the rest of Asia. This includes India, which boasts super-apps such as Paytm and the more recently launched Tata Group super-app, Tata Neu.

96. The success of super-apps is not limited to Asian markets. There are significant super-app players across Latin America and Africa, as well. *See* https://www2.deloitte.com/us/en/pages/financial-services/articles/super-apps-in-the-us.html ("So what's next in the mobile-first experience? The next evolution may be a single, one-stop-shop—the 'super app' phenomenon that has emerged and scaled across Asia, Latin America, and Africa").

The United States

97. In the United States, consumer-merchant payment innovations have been few and far between since the emergence of digital wallets, HCE, and tokenization a decade ago—innovations brought to consumers by tech pioneers, such as SimplyTapp. In the United States, there are no super-apps despite widespread recognition that the United States market potential is

huge and United States consumer interest strong.[7]

98. To become a United States super-app, the solution must provide value to help buyers replace their wallets and help sellers better interact and transact with buyers. For buyers, it must be accessible by anyone (regardless of phone type) and accepted everywhere (in stores, restaurants, online…), it must be more convenient and rewarding to use than existing wallets and standalone apps. For sellers, it must provide a universal payment, rewards and engagement tool that is accessible by any customer and accepted everywhere the seller does business, all without costly POS changes.

99. Apple Pay, Google Pay and Samsung Pay are not super-apps because they are **not accessible** to each other's users, while PayPal and Cash App are not super-apps because they are **not accepted** in most stores, malls and restaurants and cannot replace our physical wallets. None of these wallets are private self-custody wallets, where users own their own keys to have sole custody of their own data like they do for their own physical wallets. The big tech mobile wallets today also do not provide personalized payments, rewards, and engagement tools that work across existing merchant POS systems – they are too fragmented and too hard to unify across consumers and across merchants to become a United States super-app. Without a United States super-app, there is little chance for new payment rails that could challenge the pricing power of Mastercard.

[7] *See, e.g.*, S. Galloway, *Super-Apps Are Inevitable Get Ready for the First $10 Trillion Tech Company*, New York Magazine (Nov. 24, 2021), available at https://nymag.com/intelligencer/2021/11/facebook-metaverse-super-apps.html ("I'm convinced that constructing a United States super-app is the strategic-imperative of the next decade and could result in the first $10 trillion company") and https://www.pymnts.com/connectedeconomy/2022/the-data-point-72-percent-consumers-interested-super-apps/ ("[W]e surveyed nearly 10,000 consumers in Australia, Germany, the United Kingdon and the United States, finding serious appetite for one app instead of a half-dozen to navigate the pillars of the connected economy …. [¶] 'At a minimum, approximately two-thirds of respondents in all countries we surveyed reported interest in a super app,' the study stated. 'Naturally, there are subtle variations: 8% to 10% more United States respondents are 'very' or 'extremely' interested in a super app than consumers in other regions'").

100. Due to a combination of a highly-fractured banking segment (many competitive players), incompatible POS systems that only work with certain payment or rewards solutions, and far too many apps for each brand or merchant, combined with a "walled garden" approach by the big tech wallet platform providers (*e.g.*, Apple), there are significant challenges in unifying and simplifying the commerce experiences for the 250 million adults in the United States. Big tech platform providers are beholden to their fractured user base inside their "walled gardens," and financial institutions, large retailers, and telecommunication companies all compete with one another. Thus, it requires a new company that focuses on building the infrastructure for a real platform-agnostic super-app that can close the wallet and POS loop for buyers and sellers, across mobile devices, channels, and tender types.

101. A successful United States super-app provider must be dedicated to bringing consumers repeated innovations on an open platform that fosters third-party partnerships as opposed to guarding fortified fiefdoms. As a Deloitte article explained:

> Firms developing super-apps have a culture of significant transformation versus incremental change. They launch entirely new businesses regularly. They find ways to embed their app everywhere. They're able to do this by being intrapreneurial …. [¶] Successful super-apps handle partners in three ways. First, they prioritize partnership management …. Second, **super-apps create open access sandboxes for partners to develop new functionality**, which then gets plugged seamlessly into the super-app—something WeChat has done with its mini-programs. Third, super-apps maintain teams dedicated to overseeing the establishment and maintenance of partnerships.

Financial Services Super-Apps: Growth and Transformation Through Engagement, Deloitte (2022), at 8, available at https://www2.deloitte.com/us/en/pages/financial-services/articles/super-apps-in-the-us.html (emphasis added).

A Card Network Competitor

102. Super-apps bring competition into the consumer-merchant mobile wallet

contactless payments network processing space.

103. A platform-agnostic, universal super-app will support multiple payment rails. It can support not just the established card networks but also new or underutilized alternative rails, such as the Clearing House's RTP or the United States Federal Reserve's FedNow. These payment rails carry lower transaction fees compared to card payment networks. Both RTP and FedNow are real-time payment systems, payments made between bank accounts without intermediaries like card networks and acquiring banks. The existence of these United States alternative rails is not a matter of "build it and they will come." These rails, like Mastercard's, are backend infrastructure. Consumers use their virtual Mastercard credit and debit cards loaded onto mobile wallets to access Mastercard's rails. Consumers need mechanisms to access the alternative rails for consumer-merchant payments. Enter a United States super-app.

104. While a super-app can be built to permit a consumer-merchant transaction using a branded virtual credit card over the respective card network's rails, it can also be built to offer the consumer and merchant the option to sidestep the consumer's branded card and the card network's rails. In short, super-apps can both facilitate card network transactions and compete with them. Mastercard views such domestic competition as presenting an existential threat. Mastercard has reason to worry.

105. For example, in China, super-app payments are primarily transacted on non-card network rails without the use of branded cards. *See* G. Billa, Z. Aron & M. Purowitz (Deloitte Consulting LLP), *Super-Apps in Financial Services: 5 Keys to Success*, WSJ (Nov. 8, 2022), available at https://deloitte.wsj.com/cio/super-apps-in-financial-services-5-keys-to-success-01667936659 ("Throughout Asia, super-app payment solutions are already surpassing credit, debit, and cash in popularity: 92% of residents in China's major cities use WeChat or Alipay,

China's two largest super-apps, as their primary form of payment.").

106. The Chinese market is not an outlier. In 2020, Brazil's central bank rolled out a real-time payment service called PIX. Unlike its United States counterparts, PIX came with frontend functionality through, for example, requiring financial institutions over a certain size to offer it within their digital applications.[8] Credit card networks now face stiff competition in Brazil. As of 2022, a mere two years after its rollout, PIX handled a substantial share of consumer-merchant (person-to-business, P2B) transactions:

> [A]doption has exceeded expectations: … over 75% of the adult population has either sent or received a payment via PIX. While initial adoption was mostly driven by the replacement of bank wires and cash payments in a B2B / P2P context, new features added in 2021 … and growing merchant adoption have[] **led to an accelerating use for P2B transactions**. **PIX is now processing ~$250B in annualized P2B payments, equivalent to more than 40% of card volume and 20% of total consumer spend**.

See S. Rodriguez & A. Immerman, *Lessons for FedNow From Pix*, Sep. Fintech Newsletter, Andreessen Horowitz (Sep. 22, 2022), available at https://a16z.com/newsletter/paradise-fednow-how-the-2023-payments-network-will-improve-real-time-payments-september-fintech-newsletter/#lessons-for-fednow-from-pix.

107. In fact, PIX has been so successful as an alternative rail that, in 2023, its transaction volume surpassed that of credit and debit cards:

> ·A True Challenger to Credit Cards: Pix transaction for Q1 2023 totaled 8.1 billion vs. 4.2 billion credit card and 3.8 billion debit card transactions. This is the first quarter where the number of Pix transactions were more than credit and debit

[8] *See* S. Rodriguez & A. Immerman, *Lessons for FedNow From Pix*, Sep. Fintech Newsletter, Andreessen Horowitz (Sep. 22, 2022), available at https://a16z.com/newsletter/paradise-fednow-how-the-2023-payments-network-will-improve-real-time-payments-september-fintech-newsletter/#lessons-for-fednow-from-pix ("PIX requires any financial institution with 500k+ users to offer PIX within its digital application at launch" and "FedNow … added functionality will be built by its participants (vs by a central infrastructure in Brazil). While PIX evolved to be a 'front-end' solution ubiquitous to Brazilian consumers, FedNow will launch as more of a back-end network available to banks at a low operational cost").

> combined.
>
> Credit and Debit Share of Transactions has Been Declining Since Pix launched: Pix accounted for 35% of all transactions in Q1 2023, up from 23% a year ago. Credit card transactions were 18% of total, down from 20% one year ago. Debit card transactions were 16% total, down from 20%.
>
> ***
>
> Today, Pix presents a clear challenge to the credit card industry in Brazil, and it will continue to take a share from credit cards. Account-to-account instant payments facilitate an open network that solves many issues common in payments.
>
> ***
>
> United States financial institutions and card companies should be taking note. The lesson from Pix is clear: Innovation and disruption are coming.

Credit Card Transactions in Brazil May Have Peaked as Pix Continues to Surge, BusinessWire through Yahoo!Finance (Jul. 25, 2023), available at https://finance.yahoo.com/news/credit-card-transactions-brazil-may-130000365.html.

108. A United States super-app is not just about fostering payment options, it is also about lowering prices. The super-app/alternative rail system eliminates entities involved in the digital card network processing chain, including merchant acquirers and TSPs. This makes mobile wallet payments made through a super-app alternative rails system cheaper than those run through Mastercard cards on Mastercard rails (*e.g.*, a payment made using Apple Pay). For example, in Brazil, merchants pay far less for the use of PIX than they do for the use of card networks:

> Brazil's Pix retail instant payment system is 'much cheaper' than card payments for merchants, according to a paper published Wednesday by the umbrella body of the world's central banks, highlighting its growth potential for businesses after its vertiginous rise among individuals.
>
> The paper, which was co-authored by an economist at the Brazilian central bank for the Bank of International Settlements (BIS), **says Pix costs an average of 0.22% of transaction value for merchants, whereas debit cards cost slightly above 1% and credit cards reach 2.2.%** in Brazil. It is also more competitive than credit card fees on 1.7% in the United States, 1.5% in Canada and 0.3% in the European Union …. (Emphasis added).

M. Ayres, *Brazil's Pix 'Much Cheaper' Than Card Payments, Paper by Central Bank Economist*

Shows, Reuters (Mar. 23, 2022), available at https://www.reuters.com/article/brazil-cenbank-pix/brazils-pix-much-cheaper-than-card-payments-paper-by-central-bank-economists-shows-idUSL2N2VP316/ (emphasis added).

109. In short, super-apps unify the frontend experience and make the backend more efficient, while lowering transaction costs. Super-apps work and work well.

110. Mastercard understands that a successful super-app will bring competition to the United States market and may disintermediate it.

111. This takes us to OV Loop, a company founded to build a payment super-app for the United States domestic market.

V. OV LOOP

112. Mr. Graylin is a FinTech innovator and serial technology entrepreneur. He founded OV Loop in 2008, as an investor and board member, to develop a mobile communication "app." He became C.E.O. of OV Loop in 2018 to create a unified commerce platform with a "super-app" to enable payments, rewards, and engagement across devices and channels, for more frictionless commerce experiences and relationships between brands (merchants) and people (consumers).

113. Mr. Graylin served his country for more than five years as a United States Nuclear Submarine Officer. He then earned two master's degrees from MIT and holds a dozen patents for payment-related inventions. He also recently completed serving seven years on the Board of Directors for Synchrony Financials (NYSE: SYF, the largest private label credit card issuer in the world). Mr. Graylin taught part-time at MIT before COVID and is currently an MIT Connection Science Fellow with Dr. Sandy Pentland of the Media Lab. He is also an investor/director/mentor in and to numerous high-tech startups and non-profit organizations including ROCA and Global Unites.

114. Prior to becoming C.E.O. of OV Loop, Mr. Graylin was Global Co-GM of Samsung Pay, after Samsung acquired his company LoopPay, which he founded. Mr. Graylin served as Samsung Pay's Co-GM for three years. During his tenure, he helped launch Samsung Pay with LoopPay's patented MST technology and was intimately involved in working with Mastercard on Samsung Pay.

115. LoopPay created the world's first contactless digital wallet with 90%+ point-of-sale acceptance. LoopPay and Samsung Pay were at the forefront of contactless payments and created a platform that brought together issuers, merchants, and consumers that facilitated a seamless and rewarding digital wallet experience and tokenized contactless payments to over 90% of existing POS terminals.

116. Prior to LoopPay and Samsung Pay, Mr. Graylin was also the founder and former C.E.O. of ROAM Data. ROAM Data was the largest provider of mobile POS solutions for merchant service providers, including competitors of Square (Block). ROAM Data was later acquired by Ingenico, the world's largest POS terminal manufacturer.

117. Prior to ROAM, Mr. Graylin founded WAY Systems, the world's first pocket-sized mobile point-of-sale provider (acquired by Verifone); and EntitleNet, a security software company, acquired by BEA Systems to become Web Logic Enterprise Security, which later became part of Oracle.

118. Mr. Graylin is also C.E.O. at Indigo Technologies, which is delivering ultra-efficient and affordable light utility electric vehicles powered by patented road sensing smart-wheels that provide roomier, smoother, and safer ride experiences with lower carbon footprint and lower cost of ownership.

119. In short, Mr. Graylin is a storied and successful FinTech entrepreneur, who has

founded, built, and sold numerous technology companies.

120. Mr. Graylin has been leading OV Loop directly, as its C.E.O., since 2018, to create a super-app, including a multi-card digital wallet functional at B&M POS terminals. Mr. Graylin has been building OV Loop for nearly 5 years to remedy the lack of a United States super-app and introduce a super-app in this country that would work across all financial institutions, all payment networks, all tender types, and outside of the walled gardens of big tech. This vision necessarily includes the ability to perform both e-commerce and B&M transactions, and to do so completely and securely, in the best interest of the American people and the protection of their payment data.

121. Mr. Graylin has personally invested over $36 million along with more than $20 million from other shareholders in OV Loop's effort to bring United States digital payments into the modern era. OV Loop shareholders include Verizon Ventures, Lightspeed Ventures, and Star Hill Capital.

122. To further its super-app development, in June 2018, OV Loop acquired SimplyTapp. As explained above, SimplyTapp is widely credited as the originator of Host Card Emulation. The SimplyTapp acquisition added SimplyTapp's expertise and technology to OV Loop's already considerable bench of payments and security knowhow.

123. OV Loop is a fully operational company with approximately 30 employees. OV Loop developed software to implement a super-app with a full mobile wallet solution. Not satisfied with solely relying on a smartphone manufacturer to allow access to the NFC functionality on its device, and in light of the continued failure of NFC-enabled terminals to fully replace traditional terminals, OV Loop also built hardware, a key fob device, which is configured to pull tokens from the phone-based digital wallet and transmit those tokens via NFC *or* MST to B&M POS terminals. OV Loop called this hardware device the "OV Valet."

OV Valet being used for an MST purchase

OV Valet being used for an NFC purchase

Promotional image of handing OV Valet to a cashier at a retail POS

124. OV Loop's solution includes a super-app application, a TR, and its valet accessory. OV Loop built a forward-facing consumer product that includes a private wallet and messenger, with security controlled by a user's own unique key for locking their data, ID, memberships, passwords, etc., and private digital cash that shields their bank accounts and transactions, and works on virtually any smartphone at the vast majority of POS terminals across the United States *See* https://www.youtube.com/watch?v=O34l9tVRiG8 (explanatory OV Valet video);

https://www.youtube.com/watch?v=IgIBfvwgTls (explanatory OV Valet video); https://www.youtube.com/watch?v=Bq8gsrtyZ8A (explanatory OV app video).

125. In addition to developed marquee products and experienced managers, OV Loop had (and has) a waiting audience. For example, OV Loop's OV Valet beta program included over 1,000 early adopters and OV Loop's solution received positive feedback from major merchants.

126. However, just as with standard mobile wallets (*e.g.*, Samsung Wallet, Apple Pay, and Google Pay), for a super-app to be successful in the United States, it must allow its users to tap-to-pay with their existing credit and debit card accounts at physical storefronts by fetching payment tokens as a TR from TSPs. This means OV Loop needs equal access to MDES for Mastercard tokens for domestic Mastercard credit and debit cards. OV Loop has satisfied all of Mastercard's MDES requirements, but it has not been granted access to Mastercard's tokens due to the anticompetitive conduct discussed herein.

VI. OV LOOP AND MASTERCARD

127. In late 2018, OV Loop, through its C.E.O., Graylin, approached Mastercard to obtain Mastercard certification to enable Mastercard branded cards on OV Loop's super-app (the "OV Super-App"). OV Loop's discussions with Mastercard were not limited to certification. OV Loop and Mastercard also discussed OV Loop partnering with Mastercard to offer solutions to Mastercard's customers and Mastercard potentially investing in OV Loop. From the outset, Mr. Graylin told Mastercard that OV Loop was founded to build a super-app. This point was explicit in OV Loop's presentations to Mastercard and explicit on OV Loop's website.

128. For instance, Mr. Graylin's very first email to Mastercard as OV Loop's C.E.O., which was directed to Mastercard's Executive Vice President, Data, Insight & Analytics, explained that:

> Since completing my 3 year commitment to Samsung … I have **merged three different high-tech startups** with strong entrepreneurial talent and unique IP in **communications and payments**, to create a **next gen** Voice-First Conversational Commerce platform for people and businesses to better interact, transact and build better relationships. The name of the newco is OV, Inc. and we plan to stay in stealth mode until Money2020 of this year where we launch our first solution called OV Loop.
>
> We have been **busy integrating** multiple patented or patent pending **technologies in voice chats, business chats & engagement, and universal ID & payments, to launch a faster, safer chat and communications solution with digital wallet in the United States** that partners with banks and merchants to deliver more effective customer service and engagement, while accelerating the adoption of faster safer mobile payments on existing payment rails.

129. Similarly, in February 2020, Mr. Graylin met in-person with Mastercard's Executive Vice President, Digital Partnerships, Sherri Haymond, during which, among other things, Mr. Graylin and Ms. Haymond discussed integration of the OV Super-Apps' mobile wallet feature with Mastercard's MDES tokenization system. Immediately following this meeting, Mr. Graylin sent Mastercard's Ms. Haymond a presentation deck. This presentation deck was titled: "OV Loop[:] **Omni** Commerce Solutions to Win Relationships[:] Instant Credentials, Payments & Service[:] 1 Tap or Handsfree **Payment & Messaging**, **Any Device**, **Anywhere**!" The presentation deck made clear that OV Loop's product was to be multifaceted, offering customers and merchants multiple ways to connect, including through a mobile wallet feature, a bill pay feature, and a customer service messaging feature; that it was to be both device and operating system agnostic, so that, for example, it would work on both iPhones and Galaxy smartphones, on both Apple iOS and Google Android; and that it was to supplement smartphone POS terminal communication functionality with the NFC and MST enabled OV Valet, so that it could be used in more places and in different ways. The presentation deck used phrases like: "OV Omni Wallet," "Use on Any Smartphone," "Omnichannel Multimode Message & Pay," "Omnichannel Conversational Commerce Tools," "Request for Payment," "MessagePay," "OV Universal

Wallet," and "OV Concierge." Further, it explained the attributes for "Omni Wallet & Chat" as including "Omni Payment Method (In-Store, Online, In-App, In-Chat, Credit Card, ACH, RTP)" and "Omni Device & Channel (iOS, Android, PC, IPT, Auto, Calls, emails, web, app, SMS").

130. In April 2021, Mr. Graylin reiterated the multifaceted, *i.e.*, super-app nature, of the OV Loop platform to Ms. Haymond:

> We've been revamping OV Loop's platform for launch next quarter with **Multichannel Super Messenger** for brands, crypto vault based **Super Wallet** for people. I know last year Rich Clow [(Emerging Payments & Strategy Executive, Bank of America)] was not ready to support the Valet **super keychain** pilot for MDES when you called him. He and I spoke last week and as we get ready for the pilot on VTS [(Visa's tokenization system)], he said he would support us for MDES certification as well (I'm copying Rich here.) ….
>
> Separately we're also working with major insurance companies to radically lower insurance cost via **OV Super Wallet** with patent pending IOT connected car solution. **OV Super Messenger** is now integrated into Shopify for 3in1 interactive offers. We will also offer 3in1 interactive bills next quarter, debit and ACH to start, and plan to integrate RTP bill pay via **Super Messenger** by late this year (talking to Ron Shultz [(Mastercard Executive Vice President, New Payment Flows)] next week also).
>
> **Would you please help us get MDES integration and certification on your fast track?** (Emphasis added).

131. Mastercard knew exactly what OV Loop aspired to achieve, that OV Loop planned to become the first domestic super-app, and that OV Loop needed access to Mastercard's tokens as a gating item.

132. As with everyone else, absent Mastercard certification, the OV Super-App **cannot** access the Mastercard tokens for Mastercard's thousands of United States banks. This control over token access gives Mastercard the power to kill any digital platform it finds competitive or unwelcome. Unbeknownst to OV Loop then, Mastercard came to view OV Loop as a strategic threat.

133. From 2018 forward, OV Loop had dozens of meetings and calls with Mastercard,

all designed to secure the card network's approval of the OV Super-App. In all calls or meetings, Mastercard seemed enthusiastic and supportive. But, Mastercard never authorized OV Loop to go forward with Mastercard branded cards. Here is a sampling of the chronology of calls and meetings:

a. August 3, 2018: email from Will Graylin to Mohamed Abdelsadek (Subject: Time To Catch Up?)

b. December 13, 2018: email from Justin Flood to Will Graylin (Subject: Mastercard Meeting – Contact)

c. December 13, 2018: Will Graylin meeting with Mastercard

d. December 13, 2018: email from Justin Flood to Will Graylin attaching mutual NDA (Subject: RE: Mastercard Meeting – Next Steps)

e. December 19, 2018: email from Justin Flood to Will Graylin (Subject: RE: Mastercard Meeting – Next Steps)

f. December 19, 2018: email from Will Graylin to Justin Flood, John Frontz, Doug Yeager, John Ayers, Kevin Kozak, and Alejandro Imass (Subject: RE: Mastercard Meeting – Next Steps)

g. September 13, 2019: conversation between Doug Yeager and Daniela Castillo

h. September 16, 2019: email from Doug Yeager to Yannis Tsampalis, Daniela Castillo, Bruce Berger, and Hans Reisgies (Subject: connecting Mastercard + Sequent)

i. September 16, 2019: email from Hans Reisgies to Doug Yeager, Yannis Tsampalis, Daniela Castillo, and Bruce Berger (Subject: Re: connecting Mastercard + Sequent)

j. September 17, 2019: email from Hans Reisgies to Doug Yeager, Yannis Tsampalis, Daniela Castillo, and Bruce Berger (Subject: Re: connecting Mastercard + Sequent)

k. September 18, 2019: email from Bruce Berger to Daniela Castillo (Subject: Fwd: connecting Mastercard + Sequent)

l. September 18, 2019: email from Daniela Castillo to Bruce Berger (Subject: Re: connecting Mastercard + Sequent)

m. September 18, 2019: email from Bruce Berger to Daniela Castillo (Subject: Re: connecting Mastercard + Sequent)

n. September 20, 2019: email from Daniela Castillo to Bruce Berger (Subject: Re: connecting Mastercard + Sequent)

o. September 23, 2019: email from Daniela Castillo to Bruce Berger (Subject: Re: connecting Mastercard + Sequent)

p. September 25, 2019: email from Bruce Berger to Daniela Castillo attaching document with answers to recently raised questions (Subject: Re: FW: connecting Mastercard + Sequent)

q. September 26, 2019: telephone call between Bruce Berger and Daniela Castillo

r. September 27, 2019: email from Tom Fifelski to Daniela Castillo attaching documents (Subject: Requested Documents)

s. September 27, 2019: email from John Frontz to Daniela Castillo attaching financials (Subject: Re: Mastercard Application – Confidential Historical Financials)

t. October 25, 2019: email from Doug Yeager to Will Graylin copied to Mastercard (Subject: Re: FW: connecting Mastercard + Sequent)

u. October 31, 2019: email from Daniela Castillo to Doug Yeager and Will Graylin (Subject: Re: connecting Mastercard + Sequent)

v. November 11, 2019: email from Will Graylin to Daniela Castillo, Doug Yeager, and Bill Bachrach (Subject: RE: connecting Mastercard + Sequent)

w. November 12, 2019: email from to Daniela to Will Graylin, Doug Yeager, and Bill Bachrach (Subject: Re: connecting Mastercard + Sequent)

x. November 12, 2019: email from Will Graylin to Daniela Castillo, Doug Yeager, and Bill Bachrach (Subject: Re: connecting Mastercard + Sequent)

y. November 18, 2019: email from Daniela Castillo to Will Graylin (Subject: FW: connecting Mastercard + Sequent)

z. November 18, 2019: email from Will Graylin to Daniela Castillo (Subject: RE: connecting Mastercard + Sequent)

aa. November 22, 2019: email from Daniela Castillo to Will Graylin (Subject: Re:

connecting Mastercard + Sequent)

bb. November 22, 2019: email from Will Graylin to Daniela Castillo (Subject: RE: connecting Mastercard + Sequent)

cc. November 26, 2019: email from Daniela Castillo to Will Graylin (Subject: Re: connecting Mastercard + Sequent)

dd. November 26, 2019: email from Will Graylin to Daniela Castillo (Subject: RE: connecting Mastercard + Sequent)

ee. December 3, 2019: email from Daniela Castillo to Will Graylin (Subject: RE: connecting Mastercard)

ff. December 4, 2019: email from Will Graylin to Daniela Castillo attaching C-Commerce Voice Powered Omni Chat/Wallet presentation (Subject: RE: connecting Mastercard)

gg. December 12, 2019: email from Daniela Castillo to Will Graylin (Subject: FW: connecting Mastercard)

hh. December 13, 2019: Will Graylin meeting with Daniela Castillo and Yannis Tsampalis

ii. December 13, 2019: email from Will Graylin to Daniela Castillo and Yannis Tsampalis (Subject: RE: connecting Mastercard)

jj. February 1, 2020: Email from Yannis Tsampalis attaching three documents (Subject: Follow-Up – process & documentation for OV Loop)

kk. February 14, 2020: email from Will Graylin to Sherri Haymond attaching presentation (Subject: OV Loop update and Investment)

ll. February 24, 2020: email from Sherri Haymond to Will Graylin (Subject: Will<>Sherri – OV Loop update and Investment)

mm. February 26, 2020: Will Graylin meeting with Sherri Haymond

nn. February 26, 2020: email from Will Graylin to Sherri Haymond attaching presentation (Subject: Will<>Sherri – OV Loop update and Investment)

oo. March 4, 2020: email from Will Graylin to Yannis Tsampalis (Subject: Re: Follow Up – process & documentation for OV Loop)

pp. March 5, 2020: email from Yannis Tsampalis to Will Graylin (Subject: Re: Follow Up – process & documentation for OV Loop)

qq. March 6, 2020: email from Doug Yeager to Yannis Tsampalis attaching zip file (Subject: DAC paperwork)

rr. March 6, 2020: email from Will Graylin to Yannis Tsampalis (Subject: RE: Follow Up – process & documentation for OV Loop)

ss. June 24, 2020: email from Will Graylin to Rich Clow, Hans Reisgies, Joan Ziegler, Kevin Kozak, Tom Fifelski, and Sherri Haymond (Subject: RE: BofA, OV Loop & Sequent for MDES)

tt. June 25, 2020: email from Rich Clow to Will Graylin, Hans Reisgies, Joan Ziegler, Kevin Kozak, Tom Fifelski, and Sherri Haymond (Subject: RE: BofA, OV Loop & Sequent for MDES)

uu. June 25, 2020: Will Graylin meeting with Chris Kangas

vv. June 25, 2020: email from Chris Kangas to Will Graylin (Subject: hi)

ww. June 25, 2020: email from Will Graylin to Chris Kangas (Subject: RE: hi)

xx. June 29, 2020: email from Will Graylin to Chris Kangas and Sherri Haymond (Subject RE: hi)

yy. June 29, 2020: email from Tom Fifelski to Chris Kangas and Sherri Haymond (Subject: Re: hi)

zz. June 29, 2020: email from Chris Kangas to Tom Fifelski and Sherri Haymond (Subject: RE: hi)

aaa. July 2, 2020: email from Will Graylin to Chris Kangas, Tom Fifelski, Joan Ziegler, Sherri Haymond, Richard Nassar, and Kevin Kozak (Subject: RE: hi)

bbb. July 29, 2020: email from Will Graylin to Sherri Haymond and Chris Kangas (Subject: RE: BofA, OV Loop & Sequent for MDES)

ccc. August 11, 2020: email from Tom Fifelski to Charl Botes and Chris Kangas (Subject: OV/Mastercard project status)

ddd. August 25, 2020: email from Tom Fifelski to Chris Kangas (Subject: Re: OV/Mastercard project status)

eee. August 25, 2020: email form Will Graylin to Tom Fifelski and Chris Kangas (Subject: RE: OV/Mastercard project status)

fff. September 3, 2020: email from Will Graylin to Tom Fifelski, Chris Kangas,

and Charl Botes (Subject: RE: OV/Mastercard project status)

ggg. September 7, 2020: email from Will Graylin to Sherri Haymond (Subject: FW: OV/Mastercard project status)

hhh. September 21, 2020: email from Will Graylin to Chris Kangas, Charl Botes, and Sherri Haymond (Subject: RE: OV/Mastercard project status)

iii. April 25, 2021: email from Will Graylin to Sherri Haymond (Subject: OV Loop & BofA POC on MDES)

jjj. April 25, 2021: email from Sherri Haymond to Will Graylin (Subject: Re: OV Loop & BofA POC on MDES)

kkk. April 25, 2021: email from Will Graylin to Sherri Haymond (Subject: RE: OV Loop & BofA POC on MDES)

lll. June 15, 2021: email from Will Graylin to Sherri Haymond (Subject: RE: OV Loop & BofA POC on MDES)

mmm. June 23, 2021: email from Will Graylin to Sherri Haymond (Subject: RE: OV Loop & BofA PCO on MDES)

nnn. July 22, 2021: email from Donald Chapman to Thyda Chhuan (Subject: Fwd: OV Loop & BofA POC on MDES)

ooo. July 29, 2021: email from Thyda Chhuan to Donald Chapman (Subject: RE: Fwd: OV Loop & BofA POC on MDES)

ppp. July 29, 2021: email from Donald Chapman to Thyda Chhuan (Subject: Re: Fwd: OV Loop & BofA POC on MDES - question)

qqq. August 3, 2021: email from Will Graylin to Donald Chapman and Thyda Chhuan (Subject: Re: Fwd: OV Loop & BofA POC on MDES – question)

rrr. January 12, 2022: email from Donald Chapman to Kimberly Peyton, Kevin Kozak, J. Chiu, Will Graylin, John Ayers, and Luis Silva (Subject: OV Loop demo for MA MDES)

sss. January 18, 2022: email from Kimberly Peyton to Donald Chapman, Kevin Kozak, J. Chiu, Will Graylin, John Ayers, and Luis Silva (Subject: RE: OV Loop demo for MA MDES)

ttt. January 24, 2022: email from Donald Chapman to Kimberly Peyton (Subject: Re: OV Loop demo for MA MDES)

uuu. February 10, 2022: email from Donald Chapman to Kimberly Peyton (Subject: Re: OV Loop demo for MA MDES)

vvv. February 23, 2022: email from Donald Chapman to Kimberly Peyton (Subject: Re: OV Loop demo for MA MDES)

www. February 23, 2022: email from Kimberly Peyton to Donald Chapman and Luis Silva (Subject: Re: OV Loop demo for MA MDES)

134. During OV Loop's attempts to get certified as a TR for Mastercard tokens, OV Loop completed Mastercard paperwork, provided Mastercard with requested documentation, including a third-party laboratory security report and OV Valet hardware and firmware schematics, and answered questions posed by Mastercard. OV Loop also, and consistently, pushed for access to Mastercard's mobile wallet specifications (which are non-public) and MDES testing/development environment. For example, OV Loop emailed Mastercard:

- On June 29, 2020: "we need to … get product requirements";
- On July 2, 2020: "We are looking forward to kicking it off and getting product requirements for our development and timelines. If you need anything from the OV Loop side please let me know";
- On August 11, 2020: "Can we … get the latest documentation, for TEE and NFC-Cloud base product specification to move the project forward";
- On, August 25, 2020: "What do you need from us to … get the latest documentation? Getting access to the MasterCard test environment as we work with our issuing partners is important to our timelines";
- On June 15, 2021: "since our call with you [(Mastercard)] and Rich [(Bank of America)] last month, Donald on my team has tried several times to connect with Adam regarding the MDES program for NFC without success. I hope Adam is OK. Can you advise how we can move forward with MDES as a TR?;"

- And again, on August 3, 2021: "Thank you very much for connecting us with the right folks at MDES. We are looking for Mastercard Cloud Based Payments to integrate into. We need a sandbox to test an[d] as Sherri [Haymond] had mentioned a fast-track program we certify to be a TR."

135. In response, Mastercard strung OV Loop along, through at least 2022, by saying the right things—it was excited about OV Loop and looking forward to working together—without ever saying no. For example, Mastercard told OV Loop:

- On December 13, 2018: "Thanks for coming in today and talking us through a demo of the OV platform. **We are excited** about the potential and are **looking forward to many more conversations**;"
- A year later, on December 12, 2019: "We are **very excited** for our meeting tomorrow and to finally meeting you in person. [¶] For our conversation tomorrow we would like to cover: The results of our industry and security team assessment on OV's Valet; **Potential opportunities we could explore together** in the wearable space; and OV's voice solution – It would be great if you could walk us through the live demos;"
- Four months later, on March 5, 2020: "It was great seeing you as well. **Looking forward to working together**. We will set up a call early next week and discuss the next steps;"
- Just over a year later, on April 25, 2021: "Hi Will [(OV Loop)] and Rich [(Bank of America)], and great to meet you, Donald ([OV Loop)]! [¶] Will its great to hear from you. All **sounds exciting** – I'd [(Mastercard's Ms. Haymond)] **love to hear more** and see what's possible. Let's find time for later this week – I'll bring a few other people, too. **Looking forward!**;" and
- Three months later, on July 29, 2021: "Hi Donald - I believe I found the right team to

connect you in with regarding MDES development (I was right, that this did shift from Adam Granoff in recent months)."

In fact, as late as 2022, OV Loop was still sending Mastercard requested information and giving yet another demonstration to Mastercard employees.

136. Despite these years of discussions, demonstrations, and presentations, unlike when Mr. Graylin was Global Co-GM of Samsung Pay where Samsung Pay got access and certified to MDES within about six months, OV Loop has not been able to get access to the same Mastercard token service after three-plus years of trying. Mastercard has not even given OV Loop access to its MDES development and testing environment. OV Loop came to appreciate in 2022, after years of trying, that Mastercard was not (or at least was no longer) acting in good faith, and that Mastercard was in effect refusing (and still is refusing) to certify OV Loop under MDES. This was true in mid-2020, for example, when OV Loop brought Bank of America to the discussion, and again, in Spring 2021, when Bank of America reentered the fold.

137. Mastercard has, and continues to, refuse to deal with OV Loop. As explained below, Mastercard's motives for doing so are purely anticompetitive.

VII. MASTERCARD'S MONOPOLIZATION OF THE RELEVANT MARKET AND THE RESULTING INJURY TO CONSUMERS, MERCAHNTS, AND OV LOOP

138. A company is free to refuse to deal with a competitor. This is, in fact, the essence of competition. But there is one important exception: if the party saying no has significant market power and refuses to deal for anticompetitive reasons, the refusal to deal is wrongful.

139. The merchant POS network for accepting bank card payment processing was laid over many years including for contactless card payments with standards defined by Mastercard for its network processing. If Mastercard can maintain its control over its dominant network processing as the world transitions from card payments to mobile wallet payments, and it can

continue to control which mobile wallets can be used on this merchant POS network, it can continue to maintain monopoly power over the new generation of payments–mobile wallet contactless payments–which is effectively what it did (and continues to do) between 2014 and today.

140. As detailed above, mobile wallet contactless payments at the merchant POS used to be done through secure elements that stored credentials, including permanent cryptographic keys, just like their SE-equipped plastic predecessors. A plastic card SE is controlled by the respective bank that loads the credentials, while the SE on the old paradigm phones could only receive credentials provisioned via a Trusted Security Manager (TSM) controlled by the mobile operator or phone maker. The old mobile phone model was cumbersome and hard to scale, given only one party could control the SE and TSM; thus, the old method hampered adoption of mobile wallet contactless payments. By 2014, a new paradigm—one reliant on the new methods of HCE and tokenization—emerged. This new paradigm is not reliant on SEs. It is, however, reliant on a Token Service Provider (TSP), so that whoever controls the TSP controls who can become a Token Requestor (TR), *i.e.*, who can become a mobile wallet that can receive credentials for all the thousands of Mastercard banks performing contactless payments on the merchant POS system.

141. Mastercard and Visa are the sole TSPs for providing tokens for their respective cards from banks to Apple Pay. The only way for a consumer to tap-to-pay with his or her banks' Mastercard via the consumer's iPhone is through MDES. For an Apple user, there are little to no alternatives to Mastercard and Visa for mobile wallet contactless payments.

142. Mastercard and Visa are also the sole TSPs for providing tokens for their respective cards from banks to Google and Samsung's mobile wallets. To sweeten the deal for banks to participate in Mastercard's TSP service MDES, Mastercard offered to waive its fees and

effectively made its TSP free of charge throughout 2014 and 2015 when Apple Pay, Google Pay and Samsung Pay were launched. With the three major TRs (Apple, Google, and Samsung) using MDES and VTS, there was (and is) even less incentive for banks to seek alternative TSPs—the die is cast for maintaining monopoly power for years to come. All the other TSPs and TSP technology providers, including SimplyTapp that became a wholly owned subsidiary of OV Loop, could not compete against MDES and VTS. These TSP providers were initially all vying to compete in helping banks provide mobile wallet contactless payments, but all were forced out of the TSP business, including OV Loop, such that 2019 saw its last TSP licensing revenue from its final TSP customer Royal Bank of Canada (RBC) that started paying SimplyTapp in 2013 for its TSP mobile wallet contactless payments for RBC's own app. Since mobile wallets or TRs need to get access to Mastercard tokens for their users, and Mastercard solely decides which TRs to accept and which TRs to reject, and by rejecting any TRs that may become a threat of becoming a universal wallet (*i.e.*, goes across iOS and Android devices that any consumer can use) that could become a super-app that offers competitive payment methods, Mastercard can maintain its monopoly power over consumer-merchant mobile wallet contactless payments network processing services on behalf of banks and continue to reap supracompetitive profits.

143. Mastercard's control over its tokens allows it to maintain its supracompetitive, per-transaction interchange fees in the mobile wallet space, just as it has maintained such fees for transactions utilizing traditional plastic cards.

144. Mastercard's supracompetitive prices earn it supracompetitive profits. It has a net profit margin of 45%. It charges merchants exorbitant rates; charges merchants pass onto the United States consumer.

145. Mastercard's monopoly power is insulated through high barriers to entry, including

its access to and control over the millions of Mastercard cardholders it profits from. Any mobile wallet provider attempting to enter the market who is not given access to MDES is barred from reaching the millions of consumers who cannot use a product their cards are not enabled on. This is an insurmountable barrier to entry for any payment solution and is a nearly impossible hurdle for any technology company to overcome.

146. OV Loop's technology would allow consumers to conduct transactions with merchants both using and outside of Mastercard's network for digital wallet transactions. Mastercard, with anticompetitive zeal, sacrifices revenues from the former, to prevent the latter. This it does in blatant violation of the Sherman Act.

A. Mastercard's Monopoly Power Within the Consumer-Merchant Mobile Wallet Contactless Payments Network Processing Services on Behalf of Banks

147. The first relevant product market is consumer-merchant mobile wallet contactless payments network processing services on behalf of banks, or "C-M Mobile Payment Services" for short. C-M Mobile Payment Services providers simultaneously facilitate, at a physical point-of-sale through a consumer's mobile wallet: (1) a consumer's use of a financial account with a third-party to buy a merchant's goods or services; and (2) a merchant's acceptance of the consumer's payment. The consumer financial accounts are not limited to credit accounts, but can include checking and savings accounts, for example. This product market is general purpose in nature, in that the services are provided for general purpose merchant transactions opposed to confined to transactions with a specific retailer or retail group. These services are for contactless mobile wallet payments at physical points-of-sale, *e.g.*, in-store purchases using a mobile consumer device at a merchant POS terminal via NFC, MST, or scannable QR code technologies, and not online/e-commerce transactions conducted using a mobile wallet. So, for example, Mastercard and Visa

provide services in this market through their branded virtual cards for mobile wallets transacting at a physical POS via their payment rails. Similarly, OV Loop would provide services in this market through its super-app for mobile wallets transacting at a physical POS via alternative payment rails. The likes of Apple, Google, and Samsung do not currently offer services or products in this market, as their wallet applications merely play host to Mastercard and Visa virtual cards—when a consumer initiates an in-store payment with Apple Pay on an iPhone it is the on-behalf-of card network whose branded card is chosen for the transaction that provides the relevant services. Nor do card issuers (*e.g.*, Citibank and Bank of America) participate in this market.

148. The C-M Mobile Payment Services market is well-defined and distinct. Mastercard's SEC filing underscores that Mastercard knows that the C-M Mobile Payment Services market is a separate product market, subject (potentially) to disintermediation by disruptive new technologies, *e.g.*, a super-app, as alleged below.

149. The relevant geographic market is the United States. Mastercard's SEC filing underscore the reality that the United States market is a distinct market. *See, e.g.*, Mastercard Inc.'s December 31, 2022 10K at 50-51, available at https://d18rn0p25nwr6d.cloudfront.net/CIK-0001141391/3f400cd7-b9fb- 4732-9e59-c669ea4fe0cc.pdf (breaking gross dollar volume, which "represents purchase volume plus cash volume" for Mastercard branded cards, out by the "United States" and "Worldwide less United States"); *see also id.* at 54 (explaining that "[n]o individual country, other than the United States generated more than 10% of net revenue in any such period"). The distinctness of the United States as a market is also borne out by Mastercard's United States-specific fee schedule. *Cf.* J. Lardner, *Whom Do Credit-Card-Rewards Programs Really Reward?*, Dec. 15, 2022, The New Yorker, available at https://www.newyorker.com/news/daily-comment/whom-do-credit-card-rewards-programs-really-reward ("The United States, moreover,

has the industrial world's highest swipe fees …. [⁋] This country's swipe fees average 2.25 per cent of the purchase amount, or eight times the prevailing rate in nations of the European Union"). The distinctness of the U.S. as a market is further confirmed by the simple reality that, for United States residents, Mastercard branded cards issued by foreign banks are not a meaningful substitute for Mastercard branded cards issued by United States banks.

150. The relevant market in this action is the United States C-M Mobile Payment Services market (the "First Relevant Market").

151. United States consumer-merchant mobile wallet contactless payments facilitated by a virtual card-card network rails solution are interchangeable with United States consumer-merchant mobile wallet contactless payments facilitated by a super-app-alternative rails solution, and as such, both belong in the same market, the First Relevant Market. Both solutions facilitate the same type of transaction: consumer payments, at brick-and-mortar establishments, for merchant goods or services using a consumer's mobile device, and simultaneous merchant acceptance of the payments, such that a drop in the overall price for one of them below the other would lead to the cheaper solution gaining users.

152. Peer-to-peer mobile wallet payment services, for example, those P-2-P services provided by Venmo, are not part of the First Relevant Market. The ability of a consumer to reimburse their friend for their share of a restaurant tab paid for by the friend is no substitute for a consumer's ability to pay a merchant themselves.

153. Private label mobile wallet payment services are not part of the First Relevant Market. The convenience to the consumer of having a payment solution that works at many merchants can simply not be beaten by having to carry tens or even hundreds of solutions specific to individual merchants. More, the vast majority of merchants do not offer their own mobile wallet

payment services.

154. Cash and checks are not part of the First Relevant Market. These forms of payment do not offer the speed and convince of mobile wallet payments, for example, nor do they offer immediate access to credit facilities or earn rewards. Indeed, many consumers no longer regularly carry cash or checks, and some merchants no longer accept cash or checks.

155. Plastic payment cards, both magnetic strip cards and smartcards, are no substitute for digital wallets, and so do not belong in the First Relevant Market. The card network and banking industries treat digital payments as distinct from plastic-based payments, and physical cards are not interchangeable with digital wallets from a consumer or merchant perspective. Digital wallets, for example, are more secure, with passcode and biometric security features provided through the computing devices that host them in addition to tokenization. And, digital wallets, which can accommodate multiple means of payment, *e.g.*, multiple branded virtual cards, are more convenient than physical cards, which require a consumer to carry each individual form of payment, *i.e.*, each plastic card, around in their physical wallet. In addition, the card networks have different fee schedules, including entirely new fees, for mobile wallet payments, and issue specific specifications, including mobile wallet and contactless POS terminal requirements, for mobile wallet payments.

156. E-commerce mobile wallet payments are outside of the First Relevant Market, as these payments are not interchangeable with contactless mobile wallet payments. Contactless mobile payments require physical infrastructure at a real-world store, for example NFC enabled POS terminals. More fundamentally, the vast majority of merchants do not provide mechanisms to make real time in-store payments online, and a consumer's ability to purchase a product online that is shipped to him or her is no substitute for his or her ability to transact in-store in the real

world and receive the good or service in real time.

157. The United States C-M Mobile Payment Services market is a distinct market and Mastercard possesses substantial market power, indeed monopoly power, in that market.

158. Mastercard's aggregate power across payments network processing services markets in which it participates evidences its monopoly power in the First Relevant Market. Hundreds of millions of cards in consumers' pockets are Mastercard cards. The number of Mastercard cards held by consumers far outstrips all but Visa, with American Express and Discover lagging well over a 100 million consumers each behind Mastercard. *See Visa vs. Mastercard, Here's What Investors Need to Know About These Two Credit Card Giants*, Oct. 4, 2022, available at https://www.forbes.com/sites/qai/2022/10/04/visa-vs-mastercard-heres-what-investors-need-to-know-about-these-two-credit-card-giants/?sh=5158056972d9 ("According to an August 2021 article by Shift, 335 million consumers used Visa cards compared to 200 million consumers who own a Mastercard. For comparison, Discover sits at 51.4 million and American Express at 47.5 million").

159. As of 2022, 37.5% of credit cards in circulation worldwide were Mastercard cards. *See United States Credit Card Market Share by Network & Issuer – Facts & Statistics*, Christy Rodriguez, Updated: Jan. 9, 2024, Edited by Keri Stooksbury, available at https://upgradedpoints.com/credit-cards/us-credit-card-market-share-by-network-issuer/#:~:text=Mastercard%20had%20been%20consistent%20at,over%20the%20past%205%20years, citing a Nelson Report; *see also id* ("People appear to be gradually moving towards Mastercard as its share has steadily increased over the years and it currently holds 37.5% of the cards in circulation 2022"). Measured by card network purchase volume, Mastercard's market

share was 27.41% in 2022. *See id.*, citing a Nelson Report.[9]

160. Mastercard's fees, including its fees for the First Relevant Market, are supracompetitive. Mastercard has the power to maintain high fees without ceding market share or impeding demand—its fees are above what they would be if the First Relevant Market were competitive. Mastercard's fees have more than doubled in the last decade alone, contributing to a 2021 net profit margin of 46%, stock growth over the past 5 years of 102.4%, and a revenue percentage change year-over-year ratio of 23.4% growth for 2021 over 2022. *See Visa vs. Mastercard, Here's What Investors Need to Know About These Two Credit Card Giants*, Oct. 4, 2022, available at https://www.forbes.com/sites/qai/2022/10/04/visa-vs-mastercard-heres-what-investors-need-to-know-about-these-two-credit-card-giants/?sh=5158056972d9. In contrast, Visa's stock growth and revenue change ratio for the same periods were 70.2% and 10.3% growth respectively, *see id*. The general average retail net profit stands at a mere 2.4%.

161. Mastercard's high fee driven, exorbitant rate of return is indefensible. Mastercard's costs have not skyrocketed; in fact, its costs have gone way down. *Cf.* K. Partsinevelos & C. Freda, *How Small Businesses Are Fighting Inflated Credit Card Swipe Fees*, CNBC (Published Feb. 9, 2023; Updated Feb. 9, 2023), available at https://www.cnbc.com/2023/02/09/small-businesses-credit-card-swipe-fees.html ("The Federal Reserve's biannual survey of banks debit card transaction estimates that it costs banks an average of 4 cents to process a transaction, regardless

[9] *See also* Raynor de Best, Market Share of Visa, Mastercard, American Express, Discover General Purpose Card Brands in the United States from 2007 to 2022, Based on Value of Transaction, Dec. 20, 2023, available at https://www.statista.com/statistics/279469/market-share-of-credit-card-companies-in-the-united-states-by-purchase-volume/ (putting Mastercard at 25.5% for 2022); J. Lee, Mastercard's Stock Has Outperformed Visa's Over the Past 5 years. Here's Why, May 27, 2023, available at https://www.cnbc.com/2023/05/27/how-mastercard-has-outperformed-visa.html ("[Mastercard] is the second largest card network in the U.S., accounting for more than a quarter of all purchase volume using a payment card …. [⁋] The company in May 2023 had a market cap of over $360 billion, and its shares have seen a nearly 100% gain over the past five years").

of the total ticket cost. That's down sharply from about 8 cents per transaction a decade earlier. Although the central bank does not conduct the same survey for credit card transactions, the process used for debit and credit cards are similar"). Mastercard's ability to reap immense profits by charging high fees in light of low costs demonstrates its substantial market power in payments network processing services markets, including its monopoly power in the First Relevant Market.

162. The First Relevant Market's barriers to entry are high. The lack of entrants into the space demonstrates this. The principal players in the First Relevant Market are and have been Visa and Mastercard, the two large, established U.S. card networks which have each dominated payments network processing services markets for decades.

163. There are also very real network effects at play here. People use the cards they know; the greater the number of people who use Mastercard, the harder it is for a new entrant. For example, despite years of lamenting Mastercard's high fees, an overwhelming majority of United States merchants continue to accept Mastercard branded cards; and, millions of consumers continue to use Mastercard's cards despite the costs they impose on everyday purchases. More, mobile contactless branded card payment acceptance is now widespread, despite Mastercard charging merchants more for accepting these payments versus plastic cards. To be competitive, merchants must accept Mastercard branded cards, including its virtual cards at physical points of sales through contactless mobile wallets.

164. To take another example, and as detailed above and below, to meaningfully gain traction in the United States, a competitor in the C-M Mobile Payment Services market needs to be able to offer consumers the use of the consumers' branded credit and debit cards—the cards already in consumers' pockets—through its mobile offering in addition to its competitive service. Mastercard controls which mobile wallets can access Mastercard branded cards, including through

Mastercard's mandate that tokens must be used and Mastercard's position as the token service provider for its cards. Mastercard leverages its position as the TSP for its card's tokens to control entry into the First Relevant Market, denying token access to nascent competitors. In short, not only are there significant barriers to entry, Mastercard actively (and wrongfully) erects others. Mastercard has monopoly power as demonstrated in part by its power to exclude competition.

165. Through its ability to control token access, Mastercard is not only able to prevent who it goes head-to-head with for processing fee revenue in the First Relevant Market, it is also able to control who its issuers compete with on the consumer reward program front. A central feature of a super-app is personalized consumer rewards. As a Deloitte article explained: "[t]he main pulls toward super-apps and away from native apps will likely be the ability to manage fewer accounts, transact faster through consistent payments, **save money using loyalty and rewards**, and experience a better product enabled by cross-service insights and advice." *Western Super-Apps Forecasting Disruption from a Super Trend*, Deloitte (2022), at 8, available at https://www2.deloitte.com/us/en/pages/financial-services/articles/super-apps-in-the-us.html. If super-apps were to gain traction in the United States, they would foster competition between their reward programs and those offered by branded card issuers, increasing the quality of consumer reward programs. A successful United States super-app would drive down fees while increasing rewards.

166. Mastercard's monopoly power is further demonstrated by its ability to reduce output in the First Relevant Market. As explained in more detail below, OV Loop, which Mastercard refuses to certify, can facilitate mobile wallet contactless payments and drive mobile wallet adoption in ways certified wallets such as Apple Pay cannot. Accordingly, in denying OV Loop access to MDES, Mastercard is not merely transferring transaction volume from one wallet

to another, but keeping transaction volumes lower than they otherwise would be. Moreover, the high costs Mastercard imposes on consumers through its interchange fees reduce consumer spending power—more consumer spending equates to more consumer-merchant mobile wallet contactless payment transactions. The output reductions wrought by Mastercard bring output below a competitive level.

167. Mastercard possesses monopoly power in the First Relevant Market, as demonstrated by structural characteristics of the market, including barriers to entry, Mastercard's conduct, Mastercard's market share, and other direct and circumstantial evidence, including evidence of Mastercard's actual exercise of its monopoly power.

B. Mastercard's Monopoly Power Within the Market for Point-of-Sale Universal Mobile Wallet Network Processing Using Mastercard Branded Cards

168. The second relevant market, here, is the United States market for point-of-sale universal mobile wallet payment network processing using Mastercard branded cards (the "Second Relevant Market"). This market is well-defined, distinct, and controlled by Mastercard.

169. Mastercard possesses market and monopoly power in the Second Relevant Market, as demonstrated by structural characteristics of the market, including barriers to entry, its conduct, its market share, and other direct and circumstantial evidence, including evidence of its actual exercise of that power.

170. Mastercard's monopoly power is insulated through high barriers to entry and expansion in the Second Relevant Market as Mastercard has access to and, in effect, control over the millions of Mastercard credit card users. Any mobile wallet provider attempting to enter the credit and debit card processing market who is not given access to the MDES system is effectually barred from reaching millions of consumers who cannot use a product on which their cards will not be enabled. This is an insurmountable barrier to entry for any payment solution and is a nearly

impossible hurdle for any technology company to overcome.

171. OV Loop's technology would allow customers to conduct transactions with merchants both using and outside of Mastercard's network processing for digital wallet transactions, requiring Mastercard's tokenization and detokenization authorization.

172. Further, OV Loop's platform, like Samsung Pay, Google Pay, and Apple Pay, is a mobile wallet with the capability to facilitate point-of-sale transactions using Mastercard branded cards. And, although markets that utilize a branded product in its definition, such as Mastercard, are not favored, the unique nature of the emerging mobile payment and mobile wallet industry makes such a market definition appropriate in light of its size and Mastercard's role and influence therein. Further, the market for mobile wallets capable of facilitating transactions utilizing Mastercard-branded cards is appropriate, here, as any mobile wallet needs to be able to facilitate transactions using Mastercard-branded cards to gain traction within the mobile wallet space, for the same reasons discussed above.

173. Mastercard's monopoly power within this market is demonstrated by Mastercard's use of MDES to exclude companies posing a competitive threat, such as OV Loop, from this payment system. Mastercard's exclusion of such companies is intended to ensure it maintains its monopoly power over payment processing for digital wallets. For example, through Mastercard's monopoly power in the Second Relevant Market, it is able to dictate which companies are able to compete within the market, and therefore the mobile wallet point-of-sale market, generally, because, absent MDES certification, any market participant is unable to compete.

174. Mastercard uses its dominance within the Second Relevant Market to exclude competitors from its network which it perceives as any type of threat, resulting in only three mobile wallets (Apple, Samsung, and Google). Mastercard's exclusion of nearly all participants from the

Second Relevant Market not only allows it to stifle competition within that market, but also restrains consumer choice to mobile wallets it allows within its Network.

175. Mastercard also maintains its monopoly power within the Second Relevant Market by excluding "universal" mobile wallets, such as OV Loop, that can function on iOS or Android and transfer a consumer's information if they switch operating systems. Due to the switching costs between iOS and Android, Mastercard's exclusion of universal mobile wallets from the Second Relevant Market limits consumer choice even more as iOS users will be unable to utilize any mobile wallet other than Apple Pay and Android users will only be able to use Google Pay or Samsung Pay, due to switching costs.

176. Mastercard's monopoly power within the Second Relevant Market is also demonstrated by the fact that it has only granted MDES certification, required to compete in the Second Relevant Market, to three mobile wallets compatible with United States' consumers' mobile devices. Mobile wallets are a lucrative industry and have been around for well over a decade, yet, unlike every other technological breakthrough over the past twenty years, there are only three providers within the United States—Apple Pay, Google Pay, and Samsung Pay—each of which were granted MDES certification from Mastercard.

177. Providers that Mastercard excludes from its Network, and therefore the Second Relevant Market, are never able to reach consumers, as discussed herein, due to Mastercard's exclusive control over the Second Relevant Market, thus demonstrating Mastercard's ability to keep competitors out of the Second Relevant Market, and thereby limit consumers to mobile wallets of Mastercard's choosing.

178. Mastercard possesses monopoly power in the Second Relevant Market, as demonstrated by structural characteristics of the market, including barriers to entry, Mastercard's

conduct, Mastercard's market share, and other direct and circumstantial evidence, including evidence of Mastercard's actual exercise of its monopoly power.

C. Anticompetitive Conduct.

179. Prompted by anticompetitive malice, Mastercard has denied, and continues to deny, OV Loop access to MDES. This it did, and continues to do, with an intent to destroy a nascent threat to its monopoly power, and the goal of maintaining supracompetitive payment processing prices and profits.

Mastercard Provides MDES Access to Other Mobile Wallet Operators

180. Mastercard has a long established, voluntary, and profitable course of dealing with mobile wallet providers.

181. Circa 2014, Mastercard chose to enter the market for tokenization services. As a TSP, Mastercard generates tokens for card issuers to facilitate the use of those banks' Mastercard branded virtual cards on mobile wallets. An integral part of this service is connecting mobile wallets to Mastercard's MDES, so that the tokens can be used in mobile wallet payment authorization decisions. To that end, Mastercard has granted MDES access to mobile wallet providers, including Apple, Google, and Samsung, whose wallets today are the three most widely used.

182. For example, in 2015, Samsung Pay launched with MDES access. Shortly prior to launch, Mastercard said:

> As consumers increasingly rely on their mobile devices in their everyday lives, MasterCard is pleased to partner with Samsung to bring Samsung Pay to our cardholders around the world. Using advanced tokenization technology from the MasterCard Digital Enablement Service[(MDES)], we're delivering a digital payment experience that is both simple and secure, and includes all the benefits and guarantees of a MasterCard transaction.

Samsung Announces Launch Dates for Groundbreaking Mobile Payment Service: Samsung Pay,

Samsung Newsroom, Aug. 14, 2015 (quoting a Mastercard executive), available at https://news.samsung.com/global/samsung-announces-launch-dates-for-groundbreaking-mobile-payment-service-samsung-pay; *see also Mastercard Extends Partnership with Samsung to Deliver Samsung Pay in Europe*, Samsung Newsroom, Jul. 31, 2015, available at https://news.samsung.com/global/mastercard-extends-partnership-with-samsung-to-deliver-samsung-pay-in-europe ("Earlier this year, MasterCard announced it would provide the tokenization services to Samsung Pay for its secure transactions, enabling a quick scaling connection to bank partners in the United States ….").

183. Mastercard is the TSP for its cards. Its job is to provide third-party mobile wallets with the tokens of banks that issue its cards. There are no administrative difficulties with respect to Mastercard providing this access. It is designed to do so with specifications, test environments, and dedicated personnel, and it does indeed provide such access, having done so for other mobile wallet providers. Mastercard does not have to design and implement new systems to afford OV Loop access to Mastercard's tokens.

184. Mastercard facilitates mobile wallet token access because it is good business, not because of an intervening government agency or overarching regulatory scheme that mandates that it do so. Mastercard, directly or indirectly, charges issuers and merchants/acquirers fees for its TSP services. More, Mastercard admits that continued success and expansion in digital payments, such as mobile wallets, is critical to its bottom line.

By Denying OV Loop MDES Access, Mastercard Forgoes Short-Term Profits for Long-Term Anticompetitive Gain

185. More MDES-certified mobile wallets in the hands of consumers means more digital interchange revenue for Mastercard, plus reduced fraud costs, given mobile wallets' enhanced security features. In refusing OV Loop MDES access, Mastercard is foregoing profit generated

through mobile wallet transactions. In refusing OV Loop MDES access, Mastercard is denying a mobile wallet access to the very system Mastercard set up to service mobile wallets to drive Mastercard digital payment revenue in the first place.

186. OV Loop's solution will drive token use that is unserved by the mobile wallets Mastercard has certified to MDES.

187. OV Loop is the **only** universal mobile wallet provider across iOS and Android offering MST devices in the United States.[10] This means that OV Loop's solution can be used by virtually any consumer and used at the substantial number of merchants with non-NFC enabled POS terminals that remain in use in this country: from millions of small restaurants and stores to the largest of retailers like Walmart. From a profit and security perspective, it is irrational for Mastercard to want to leave these legacy terminals unserved by a mobile wallet, as that leaves them unserved and unsecured by its tokenization service.

188. OV Loop's MST device is the OV Valet. The OV Valet's form factor, essentially a key fob, gives OV Loop's solution another advantage over the mobile wallet providers Mastercard has connected to MDES. At many B&M establishments, for example, restaurants, credit and debit card payments are made by handing the card off to a merchant's employee, who then runs the card outside of the presence of the cardholder. Understandably, the average consumer is not willing to hand over their smartphone to a person they do not know, or take their wearable off of their wrist, to make a purchase. Instead, and quite sensibly, the consumer defaults to their virtual card's less secure plastic counterpart to make the payment. Here, too, by not

[10] Apple iPhones, Google Pixel phones, and Garmin smartwatches were never MST enabled. LG offered a magnetic emulation technology, but LG no longer makes phones. Samsung launched Samsung Pay on MST enabled Galaxy phones. But, given NFC and MST present separate phone component costs, the fact that NFC enabled POS terminals have reached a sizable level of penetration, and the fact that Samsung does not make money off of Samsung Pay, but rather phone sales, Samsung stopped releasing MST enabled devices in the United States

enabling OV Loop's solution, Mastercard is failing to grow its digital business.

189. These missed, higher margin, tokenization opportunities are not fringe cases. 30% of millions of terminals remain non-NFC enabled—many of them "mom & pop" retailers. In 2019, for example, it was estimated that nearly 50% of small to medium business terminals remained non-NFC enabled. And, "dining" is a major retail category. But OV Loop's wallet is not just about missed use cases, it is about overall mobile payment adoption. More consumers will make the switch to digital payments when they are confident that they can truly leave their physical wallet at home; when they can rest assured that they can use their virtual card where and how they want. In refusing OV Loop MDES access, Mastercard is not just forsaking profits, but stalling the growth of a segment it views as its strategic imperative to grow.

190. Mastercard's apparent shortsightedness as a TSP and network can only be explained by a larger anticompetitive scheme to maintain a stranglehold on the market for consumer-merchant mobile wallet contactless payments network processing services on behalf of banks. Mastercard refuses to give OV Loop what it needs to compete against the likes of Apple Pay as a mobile wallet today, because Mastercard is bent on preventing the emergence of super-app-alternative rail transactions tomorrow, transactions that would compete with Mastercard virtual card-Mastercard rail transactions.

Mastercard's Conduct Towards OV Loop, a Nascent Threat To Its Monopoly Power, Is Discriminatory

191. OV Loop merely seeks access to MDES in kind with Samsung, Apple, and Google. Mastercard has discriminated against OV Loop in denying OV Loop that access.

192. OV Loop's solution is just as secure as Samsung Pay/Wallet, Apple Pay, Google Pay, and Garmin Pay, and OV Loop is not some two-bit-player not worth Mastercard's time.

193. OV Loop is staffed with experts in payment and security technology. Its C.E.O.,

Mr. Graylin, founded a security software company that is now part of Oracle, worked on POS technologies, developed MST, worked with Mastercard on Samsung Pay certification to MDES, and launched Samsung Pay. OV Loop uses HCE technology developed by the originator of HCE, SimplyTapp, and Mastercard engaged with OV Loop's now subsidiary, SimplyTapp, on HCE adoption and proliferation. Mr. Graylin and SimplyTapp are known players to Mastercard and the industry at large; players that Mastercard used to work with but now with which it refuses to work. The OV Valet uses the same MST technology that the original Samsung Pay used at launch. OV Loop's solution uses HCE, just as other mobile wallets certified by Mastercard. And the OV Loop solution opens up revenue streams and drives mobile wallet adoption in ways other wallets do not. Yet, Mastercard has granted MDES access to companies with no prior payment technology experience, like Apple and Garmin, but will not provide the same to OV Loop.

194. Tellingly, Mastercard will not even give OV Loop access to its mobile wallet specifications or its testing environment, something it readily did for Samsung (and others). There is no legal business justification for Mastercard's refusals; rather, Mastercard refuses to deal with OV Loop, because OV Loop, unlike the mobile wallets Mastercard certified, is a nascent threat to its monopoly power.

195. Mastercard refused OV Loop MDES access to prevent it from gaining traction with consumers, because OV Loop's mobile wallet is part of a universal super-app platform, while the likes of Apple Pay, Google Pay, and Samsung Pay are not. The current MDES certified mobile wallets do not merge payments, messaging, and rewards, for example, into a single application. Nor are Apple, Google, and Samsung concerned with liberalizing consumer-merchant payments.[11]

[11] Indeed, Apple reached an agreement with issuing banks, that in exchange for fees paid to Apple for certain payments made with Apple Pay, Apple would not attempt to develop its own credit card network to compete with Mastercard and Visa.

Apple Pay and Samsung Pay are features meant to drive smartphone sales. And, in this country, Google, without offering a super-app, already occupies the position successful super-apps occupy in other countries: its search engine serves as a user's entry point onto the web. These established tech companies are beholden to their walled ecosystems and safeguarding their current business models. They are not even universal mobile wallets much less universal super-apps. For example, Samsung Wallet and Apple Pay only work on Samsung and Apple manufactured devices respectively, and you cannot use Google Pay to tap-to-pay at brick-and-mortar stores on an iPhone.

196. In contrast, the OV Super-App provides not just a mobile wallet but, for example, a universal commerce tool that lets merchants directly engage with and reward customers in-stores and online. The OV Super-App also, for example, gives consumers control over the encryption keys used to safeguard their private information, so that consumers can choose which brands to share what data with, providing consumers with increased privacy and merchants with increased customer loyalty. In further contrast to the MDES certified wallets, the OV Super-App can be used on any device and on any operating system. It works at B&M locations on Android phones through both the phone's built-in NFC functionality and the OV Valet and on Apple iPhones through the OV Valet. The OV Loop solution is a payment app, a messaging app, a rewards and engagement app, and more; it is a super-app, not just a mobile wallet. OV Loop's solution helps consumers and merchants build more direct and trusted commerce relationships across channels, devices, and tender types.

197. Mastercard views OV Loop as a super-app developer, and therefore a competitive threat. As explained above, Mastercard fears that a universal super-app will drive not just wider mobile payment adoption but non-credit/debit card mobile payment adoption through super-app-alternative rail payments. In this way, OV Loop, unlike the certified wallets, will compete for

Mastercard's card processing fee revenue. OV Loop would collect a fee for processing alterative rail transactions that would be split between it and the alternative rail entity, *e.g.*, the Clearing House, opposed to the acquiring merchant collecting a fee on behalf of a card network, *e.g.*, Mastercard. The OV Loop fee would be more competitive than what Mastercard charges, given, as explained above, a super-app-alternative rail transaction involves fewer players than a virtual card-card network transaction. The super-app-alternative rail transaction is more efficient. More, Mastercard fears that super-app-alternative rail transactions, which do not need a TSP, will reduce its interchange fee revenues.

198. In the end, Mastercard fears not just price competition from OV Loop, but the disintermediation of the card networks. Mastercard believes that its current United States business model may be disintermediated by United States super-apps that achieve scale, which is the way the card model is headed in Brazil, and the fate it suffered in China. As Mastercard put it in its 2022 10K filing with the United States Securities and Exchange Commission:

> **Competition**[:] …. **Alternative Payments Systems and New Entrants** …. Many of these providers, who in many circumstances can also be our partners or customers, have developed payments systems focused on online activity in **e-commerce and mobile channels** (in some cases, expanding to other channels), and may process payments using in-house account transfers, **real-time account-based payments networks** or global or local networks. Examples include digital wallet providers (such as **Paytm**, PayPal, **Alipay** and Amazon), point of sale financing/buy-now-pay-later providers (such as Klarna, Affirm and Afterpay), mobile operator services, mobile phone-based money transfer and microfinancing services (such as M-PESA) and handset manufacturers.
> ***
> **Disintermediation** from stakeholders both within and outside of the payments value chain could harm our business …. Although we partner with fintechs and technology companies (such as digital players and mobile providers) that leverage our technology, platforms and networks to deliver their products, **they could develop platforms or networks that disintermediate us from digital payments and impact our ability to compete in the digital economy**. These companies may also develop products or services that compete with our customers within the payments ecosystem and, as a result, could diminish demand for our products and services.

Mastercard Inc.'s December 31, 2022 10K at 21 & 30, available at https://d18rn0p25nwr6d.cloudfront.net/CIK-0001141391/3f400cd7-b9fb-4732-9e59c669ea4fe0cc.pdf.

199. Visa has expressed the same concern:

> "Business Risks[:] We face intense competition in our industry …. Some of our **competitors**, including … certain **alternative payments systems like Alipay and WeChat Pay**, operate closed-loop payments systems, with direct connections to both merchants and consumers …. We also run the risk of disintermediation due to factors such as emerging technologies and platforms, including mobile payments …. We expect the competitive landscape to continue to shift and evolve. For example: …. [W]e, along with our competitors, clients, network participants, and others are **developing or participating in alternative payments systems or products, such as mobile payment services … that could either reduce our role or otherwise disintermediate us from the transaction processing or the value added services we provide to support such processing** …. [P]arties that access our payment credentials, tokens and technologies, including clients, technology solution providers or others might be able to migrate or steer account holders and other clients to alternative payment methods or use our payment credentials, tokens and technologies to establish or help bolster alternate payment methods and platforms …. Our business could be harmed if we are not able to maintain and enhance our brand, if events occur that have the potential to damage our brand or reputation, or if we experience brand disintermediation …. The popularity of products that we have developed in partnership with technology companies and financial institutions may have the potential to cause brand disintermediation at the point of sale and decrease the presence of our brand.

Visa Inc., Form 10-K for Fiscal Year ended Sep. 30, 2022 at 21-24, available at https://www.sec.gov/Archives/edgar/data/1403161/000140316122000081/v-20220930.htm; *see also id*. at 14 ("COMPETITION[:] …. Digital Wallet Providers: They continue to expand payment capabilities in person and online for consumers and merchants. While digital wallets can help drive Visa volumes, they can also be funded by non-card payment options").

200. By excluding OV Loop, Mastercard is able to maintain its supracompetitive interchange fees to the detriment of consumers and merchants. In refusing to deal with OV Loop, Mastercard has willfully acted to exclude competition to maintain (or attempt to obtain) a

monopoly—not for legitimate business purposes. Mastercard understands that, in order for OV Loop to establish itself with consumers, OV Loop must first gain traction with consumers and merchants through the established United States card payment system. Mastercard said as much about emerging alternative payment systems in its own 10K filing:

> Although we partner with fintechs and technology companies (such as digital players and mobile providers) **that leverage our** technology, platforms and **networks** to deliver their products, **they could develop platforms or networks that disintermediate us** from digital payments and impact our ability to compete in the digital economy.

Mastercard Inc.'s December 31, 2022 10K at 21 & 30, available at https://d18rn0p25nwr6d.cloudfront.net/CIK-0001141391/3f400cd7-b9fb-4732-9e59c669ea4fe0cc.pdf. As did Visa:

> [P]arties that access our payment credentials, tokens and technologies, including clients, technology solution providers or others might be able to migrate or steer account holders and other clients to alternative payment methods or **use our payment credentials, tokens and technologies to establish or help bolster alternate payment methods and platforms** ….

Visa Inc., Form 10-K for Fiscal Year ended Sep. 30, 2022 at 21-24, available at https://www.sec.gov/Archives/edgar/data/1403161/000140316122000081/v-20220930.htm.

201. Mastercard's use of MDES to exclude companies posing a competitive threat, such as OV Loop, from the United States card payment system is intended to ensure it maintains its monopoly power. Mastercard denied and continues to deny OV Loop MDES access with the anticompetitive intent of destroying OV Loop, and thus eliminating a competitive threat to its dominance over digital payments.

MDES is an Essential Facility Denied to OV Loop

202. Mastercard's MDES is an essential facility with respect to participation in the United States consumer-merchant mobile wallet contactless payments network processing services

on behalf of banks' market. In order for OV Loop to meaningfully compete as a universal mobile wallet it needs MDES access.

203. Consumers do not want to have to sign-up for a new card to use a mobile wallet; they want to use the cards they already have in their physical wallets on their mobile devices. OV Loop heard this time and again from its early adopters. For example, as one early OV Loop user put it:

> Was so excited to finally get to download the app today. I upgraded the loop and **added a … Mastercard immediately** and noticed it stated it was only good for online purchases. Then I noticed the email that I received and was REALLY disappointed to discover that I couldn't add either of the cards to the actual loop fob …. **I can't believe all of the time that your team had to work out agreements with … MasterCard and now we have it in our hands and can't use it**.
>
> I do like the construction of the loop. It seems really solid …. The update process went very smooth as well. The app is very easy to navigate and is very polished.
>
> Still, **so disappointed that I've waited all this time for manufacturing and shipping only to now have to wait another unknown period of time before I can actually use it**.

204. As another OV Loop early adopter explained:

> When I saw your campaign way back when, I was excited about the functionality of your product. I believe I'm an early bird contributor … and bought 2 OV Valet's ….
>
> My top two credit/debit cards were "Not eligible for Valet" …. One was with the credit union that I have dealt with for 30 years (American Heritage Federal Credit Union) which I could understand may not be eligible in the early stages of your product launch. **The second one was Citi Mastercard. This one I do not understand. This is a major, top credit card company and to come up as "Not eligible for Valet" was very concerning**.
> ***
> 1. …. **Citi Mastercard…how are they not eligible for Valet? When will they be added? If these can be added, my experience may be salvageable**.
> 2. Provide a full refund to me.

205. And as yet another OV Loop user more colorfully put it:

> I live in the US. I purchased an OV Valet. I was hoping to enjoy the convenience

> of not having to pull out my card when making a purchase. I loaded my OV Valet with my 2 cards and went to use it to pay for lunch and it didn't work. I checked the app on my phone and saw this message: "Not eligible for Valet." WTF!!!! Please provide some information why.

206. Given the dominance of Mastercard and Visa branded cards, in order for a mobile wallet to meaningfully compete, it must work with *both* Mastercard and Visa virtual cards. Given Mastercard and Visa mandate the use of tokens for mobile wallets using their virtual cards, there is no alternative to using tokens for Mastercard/Visa branded card mobile wallet payments. Since Mastercard and Visa are the custodians of their banks' tokens for their respective virtual cards, the only way for a mobile wallet to work with a Mastercard card is through Mastercard's tokenization system, MDES, and similarly, through Visa's tokenization service, VTS, for a Visa card. For a mobile wallet provider, VTS is not a substitute for MDES, as MDES is the only infrastructure for accessing the tokens for Mastercard's virtual cards. MDES is an essential facility.

207. It is not feasible for OV Loop to replicate MDES by entering the tokenization market as a TSP for Mastercard branded cards. To do so, OV Loop would have to supplant Mastercard as the TSP for its own cards. This would entail getting thousands of banks to integrate with OV Loop for provisioning tokens for the Mastercard branded cards they issue. A decade into tokenization, the structural barriers and capital expenditures of competing with Mastercard as a TSP for its own cards are too high. The banks have entrenched relationships with Mastercard, using its cards and its card network in addition to MDES. In addition, the banks have made investments in their backend infrastructure to connect it with MDES. The banks have no incentive to switch, much less switch en masse.

208. As explained above, Mastercard granting OV Loop MDES access is more than feasible. Mastercard is in the business of providing mobile wallets with tokens for its bank issuers.

209. Without MDES, OV Loop is unable to functionally compete as a mobile wallet and

super-app. This is Mastercard's intent. In the United States, debit and credit cards are the digital payment norm. In order to gain traction in the United States' market, a super-app's mobile wallet feature **must** be able to facilitate debit and credit card payments at existing POS terminals. The super-app must be able to compete with Apple Pay, Samsung Pay, and Google Pay to be "super." If it cannot do that, then it cannot effectively migrate consumer payment behavior from branded cards and conventional mobile wallets to a super-app, and achieve the scale needed to transition to an entirely new consumer-merchant payment system–the super-app-alternative rail system–to provide consumers and merchants with a choice in digital consumer-merchant payments. Mastercard refuses to provide OV Loop access to MDES in order to kill OV Loop's ability to achieve widespread adoption of its platform with the end goal of thwarting the rise of a competing payment system and preserving its monopoly.

D. Antitrust Injury.

210. OV Loop has been injured-in-fact, directly, by Mastercard's anticompetitive conduct.

211. Mastercard's conduct—a refusal to deal and a denial of access to an essential facility—is a material cause of the harm OV Loop has sustained. Mastercard's refusal to grant OV Loop access to MDES has thwarted OV Loop's efforts to establish a United States super-app. It has angered OV Loop's earlier consumer adopters, lost OV Loop both consumer and merchant users, lost OV Loop partnerships with the likes of banks and merchants, and caused OV Loop significant damages, including lost profits, lost opportunities, and diminished resources. OV Loop is funded; the OV Super-App and OV Valet are developed; and OV Loop boasts of management with deep expertise. It is ready to go; it is ready to bring a super-app to the United States consumer and foster choice through the development of a super-app-alternative payment rails consumer-

merchant solution. Mastercard's conduct, which renders the tap-to-pay mobile wallet feature of the OV Super-App functionally useless to the customers of thousands of United States banks, has caused significant damage and anticompetitive injury to OV Loop.

212. The harm sustained by OV Loop is exactly the kind that Congress sought to remedy with the antitrust laws. OV Loop's injury is an antitrust injury.

213. It is, of course, true that the antitrust laws protect competition rather than competitors. Here, however, OV Loop, and its development of a super-app generally, is the very competition Mastercard is attempting to thwart by refusing to deal and denying access to an essential facility. Mastercard's conduct is exclusionary and aimed at OV Loop. Mastercard seeks to exclude OV Loop, a promising competitor, from the consumer-merchant mobile wallet contactless payments network processing services on behalf of banks' market, so that Mastercard can prevent super-app-alternative rail competition and maintain its monopoly. It is as a result of this anticompetitive conduct that OV Loop has been injured.

214. The same Mastercard conduct that injures OV Loop injures competition and the United States consumer.

215. Mastercard reaps massive profits by charging merchants processing fees. These fees are supracompetitive. The network Mastercard uses, on behalf of banks, to process consumer-merchant mobile wallet contactless payments—a new form of digital payments—is the same, long-established network it uses and has used for decades to process magnetic stripe plastic card payments. This is a simple and longstanding technology. It in no way merits the 50% returns Mastercard receives in the present world. Nor does it merit the doubling in processing fees that the last decade has seen. *See* Freda & K. Partsinevelos, *The Fight Over a Bill Targeting Credit Card Fees Pits Payment Companies Against Retailers*, CNBC (Published Jul. 20, 2023; updated

Aug. 1 2023), available at https://www.cnbc.com/2023/07/30/credit-card-fee-fight-pits-payment-companies-against-retailers.html ("Swipe fees … have more than doubled in the past decade, hitting a record $160.7 billion in 2022, according to the Nilson Report. On average, United States credit card swipe fees account for 2.2% of a transaction, according to the Merchants Payments Coalition"). Mastercard gets these returns because it has barred all others who might compete, now or prospectively, including OV Loop. This is detrimental to the consumer.

216. Mastercard's fees are a major merchant cost with card fees being a top operating expense for major retailers and small business alike. For example, according to the Texas Restaurant Association, credit card fees are, on average, the third-highest restaurant operating expense. *See* K. Partsinevelos & C. Freda, *How Small Businesses Are Fighting Inflated Credit Card Swipe Fees*, CNBC (Published Feb. 9, 2023; Updated Feb. 9, 2023), available at https://www.cnbc.com/2023/02/09/small-businesses-credit-card-swipe-fees.html.

Unsurprisingly, merchants pass this substantial tax of doing business onto their customers, the American consumer, typically as a charge built into the advertised price. *See* C. Freda & K. Partsinevelos, *The Fight Over a Bill Targeting Credit Card Fees Pits Payment Companies Against Retailers*, CNBC (Published Jul. 20, 2023; updated Aug. 1 2023), available at https://www.cnbc.com/2023/07/30/credit-card-fee-fight-pits-payment-companies-against-retailers.html ("Swipe fees are often built into the price consumers pay for goods and services ….").[12] The added cost levied on the consumer as result of card fees is not trivial. In 2021, one estimate put it at $900:

> Many small businesses feel they have little choice but to pass on the fees to consumers via higher prices or risk smaller profit margins. Swipe fees drove up prices for the average American by at least $900 in 2021, according to estimates from the Merchants Payments Coalition, which represents a variety of small

[12] These same consumers are, of course, already paying issuers annual credit card fees, bank service fees, and interest payments.

businesses including restaurants and convenience stores.

K. Partsinevelos & C. Freda, *How Small Businesses Are Fighting Inflated Credit Card Swipe Fees*, CNBC (Published Feb. 9, 2023; Updated Feb. 9, 2023), available at https://www.cnbc.com/2023/02/09/small-businesses-credit-card-swipe-fees.html.

217. In refusing OV Loop MDES access and preventing the head-to-head competition between virtual card-card network payments and super-app-alternative rail payments, Mastercard is charging United States consumers ever increasing costs, including costs added on to basic retail items like groceries (cost consumers can ill afford in these inflationary times). As the president of major ecommerce software provider, Shopify, commented:

> Interchange fees are effectively a tax on commerce, …. We began to notice that these fees kept climbing and climbing and climbing, and we felt that something was up …. [⁋] Relative to every other country Shopify operates in, interchange fees are highest in America.

C. Freda & K. Partsinevelos, *The Fight Over a Bill Targeting Credit Card Fees Pits Payment Companies Against Retailers*, CNBC (Published Jul. 20, 2023; updated Aug. 1 2023), available at https://www.cnbc.com/2023/07/30/credit-card-fee-fight-pits-payment-companies-against-retailers.html.

218. Mastercard's conduct also increases costs to the consumer in another important way. As explained above, OV Loop's solution can facilitate transactions that the mobile wallets already certified by Mastercard to MDES cannot, and OV Loop's wallet can drive digital payment adoption in ways the MDES certified wallets cannot. By not certifying OV Loop, Mastercard is reducing digital transaction output, *i.e.*, there are fewer digital transactions than there would be with OV Loop on MDES. Mastercard's anticompetitive conduct thus leaves large swaths of consumer transactions unsecured by tokenization. The resulting fraud is a major cost to merchants and banks, another cost they pass onto the American consumer.

219. But the injury to the consumer does not stop with the increased costs of goods and services wrought by Mastercard's fees. Mastercard's conduct is stifling innovation, leaving the United States consumer (and merchant) in a forgone age, while consumers (and merchants) living in countries like Brazil enjoy services they do not. The United States consumer is left not just with a lack of choice in how to make digital payments to merchants, but with poorer quality applications that lack the features and conveniences of their foreign counterparts. The harm Mastercard has caused the United States consumer, merchants, OV Loop, and competition-at-large must be remedied.

VIII. THE CLAIMS

CLAIM I
(Violation of Section 2 of the Sherman Act: Unlawful Monopolization Through Refusal to Deal)

220. OV Loop realleges and incorporates by reference the allegations set forth in the paragraphs above.

221. Mastercard has engaged in conduct violative of Section 2 of the Sherman Act, which "prohibits the "monopoliz[ation of] any part of the trade or commerce among the several States, or with foreign nations." 15 U.S.C. § 2.

222. As described above, Mastercard possesses monopoly power in the First Relevant Market, a valid antitrust market. Mastercard has possessed this monopoly power at all times with respect to the conduct complained of herein.

223. Mastercard has willfully acquired, maintained, and/or continues to maintain its monopoly power in the First Relevant Market, as distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident. Put differently, Mastercard has engaged in, and continues to engage in, exclusionary, anticompetitive conduct.

224. Mastercard's anticompetitive conduct comes in the form of a willful refusal to deal with OV Loop based on Mastercard's anticompetitive malice. For example, without a legitimate business justification or any procompetitive benefits, Mastercard denied OV Loop access to MDES. Mastercard has denied OV Loop MDES access because Mastercard fears OV Loop as a competitor in the First Relevant Market. There is no rational explanation for Mastercard's conduct, absent a specific intent to harm competition and achieve an anticompetitive effect. Mastercard's intent is to limit OV Loop's ability to gain traction as a super-app and thereby prevent OV Loop from offering a solution—a super-app-alternative network payment system—that will compete directly with Mastercard's virtual card-card network payment system. Mastercard has acted to hamstring OV Loop so that Mastercard can reap supracompetitive profits, including profits from processing fees. Mastercard has achieved its aims and continues to achieve its aims through its refusal to deal, which prevents the development of a competing super-app-alternative network payment system and maintains Mastercard's supracompetitive fees.

225. Evidence of Mastercard's exclusionary conduct comes in several forms. For example, in refusing OV Loop access to MDES, Mastercard has acted contrary to its long-established business practice of granting mobile wallet providers access to MDES so that they can host the tokens for the virtual cards of Mastercard's thousands of United States banks on their wallets. Mastercard has granted such access to the likes of Apple, Samsung, Google, LG, and Garmin for their respective mobile wallets. There are no administrative difficulties with respect to Mastercard doing the same for OV Loop. As described above, Mastercard is in the business of providing such access, as a token service provider. Nor are there any legitimate business justifications for denying OV Loop MDES access. For example, OV Loop's solution—which is built by well-known payment experts that worked on widely implemented payment features,

including Host Card Emulation, and on a mobile wallet Mastercard has certified to MDES, Samsung Pay—is just as secure as certified wallets.

226. A further example of Mastercard's anticompetitive conduct comes in the form of it forsaking short-term profits in refusing to deal with OV Loop. OV Loop's solution, for example, reaches use cases that the mobile wallets Mastercard has certified to MDES cannot, and OV Loop's wallet can drive digital payment adoption in ways the certified wallets cannot. In denying OV Loop MDES access, Mastercard is losing interchange fees it would generate through OV Loop's mobile wallet and is foregoing an opportunity to grow a business it has identified as important to its bottom line. Moreover, Mastercard is forsaking the procompetitive effects—increased security and thereby lower consumer fraud costs—afforded by its own tokenization service in refusing OV Loop MDES access.

227. Mastercard's refusal to deal with OV Loop is part of a larger anticompetitive enterprise to exclude super-apps from the First Relevant Market. Mastercard refuses OV Loop MDES access to prevent OV Loop from leveraging its payment application into a super-app-alternative rails payment system, through which OV Loop would compete for Mastercard's United States payment processing revenue. Mastercard's conduct violates its duty under Section 2 of the Sherman Act to compete fairly within the United States by not forgoing short term profits for the purpose of blocking competition and to knowingly acquire and/or maintain a monopoly. Mastercard's anticompetitive conduct in the First Relevant Market has had, and continues to have, a substantial impact on interstate commerce.

228. As a direct and proximate result of Mastercard's exclusionary conduct, OV Loop has suffered injury to its business, including through hindrance of its full-scale deployment of the OV Super-App and OV Valet, which has resulted in lost profits and lost opportunities, for example.

Mastercard's anticompetitive conduct has drastically limited OV Loop's ability to earn revenue and gain traction as a mobile wallet and super-app. OV Loop has suffered damage in an amount to be determined at trial.

229. OV Loop's injury is the type of injury the antitrust laws were designed to prevent and flows from that which makes Mastercard's conduct unlawful. Mastercard's exclusionary acts and acquisition and/or maintenance of its monopoly have caused substantial anticompetitive effects in the First Relevant Market, including increased prices and costs to consumers, as well as reduced innovation. OV Loop's suffered injuries are both injuries-in-fact and antitrust injuries and stem directly from Mastercard's refusal to deal with OV Loop. The injury Mastercard has caused and continues to cause OV Loop is a foreseeable consequence of Mastercard's anticompetitive and unlawful conduct.

230. As a result of Mastercard's anticompetitive conduct, OV Loop has been damaged, and will continue to be damaged, until Mastercard is enjoined from discriminating against OV Loop based on Mastercard's anticompetitive intent. Mastercard has acquired and maintained, and if not restrained by this Court will continue to maintain, its monopoly power in the First Relevant Market to the detriment of competition and the United States consumer.

231. Mastercard will continue its anticompetitive conduct, which is directed towards OV Loop as well as similar companies posing a competitive threat to Mastercard's monopoly power over transactional fees, and harms competition in the First Relevant Market and consumers, unless enjoined by this Court. OV Loop faces real, substantial, and irreparable damage and injury of a continuing nature, as does competition in the First Relevant Market, from Mastercard's refusal to allow OV Loop access to MDES similar in kind to that which it provides the likes of Apple, Samsung, Google, and Garmin. OV Loop has no adequate remedy at law for this damage.

CLAIM II
(Violation of Section 2 of the Sherman Act: Attempt to Monopolize by Refusal to Deal)

232. OV Loop realleges and incorporates by reference the allegations set forth in the paragraphs above.

233. In violation of Section 2 of the Sherman Act, Mastercard has attempted to, and is continuing to attempt to, willfully and wrongfully acquire and possess monopoly power in the First Relevant Market. Mastercard has engaged in exclusionary, anticompetitive conduct with the specific intent to monopolize the First Relevant Market with a dangerous probability of achieving monopoly power in said market.

234. Mastercard possesses a dangerous probability of achieving monopoly power in the First Relevant Market. For example: Mastercard commands a substantial share of the First Relevant Market; has been found to have engaged in anticompetitive conduct in other payments network processing services markets; benefits from network effects that it leverages through its control over the tokens for thousands of banks to keep competitors out of the First Relevant Market; has been able to impose higher margin fees and new fees in the First Relevant Market without losing market share; and is attempting to monopolize a market with significant barriers to entry. Mastercard's scheme to monopolize the First Relevant Market has had success in foreclosing competition, and Mastercard has possessed the dangerous probability of achieving monopoly power at all times with respect to the conduct complained of herein.

235. Mastercard's anticompetitive conduct comes in the form of a willful refusal to deal with OV Loop based on Mastercard's anticompetitive malice. For example, without a legitimate business justification or any procompetitive benefits, Mastercard has denied OV Loop access to MDES. Mastercard has denied OV Loop MDES access because Mastercard fears OV Loop as a

competitor in the First Relevant Market. There is no rational explanation for Mastercard's conduct, absent Mastercard's specific intent to harm competition and achieve an anticompetitive result. Mastercard's intent is to prohibit OV Loop's ability to function as a super-app and thereby prevent OV Loop from offering a solution—a super-app-alternative network payment system—that will prevent Mastercard from establishing a monopoly through direct competition with Mastercard's virtual card-card network payment system. Mastercard has acted to hamstring OV Loop so that Mastercard can reap supracompetitive profits, including profits from processing fees. Mastercard's continued refusal to deal with OV Loop affords Mastercard a dangerous probability of achieving its aims, the monopolization of the First Relevant Market.

236. Evidence of Mastercard's exclusionary conduct comes in several forms. For example, in refusing OV Loop access to MDES, Mastercard has acted contrary to its long-established business practice of granting mobile wallet providers access to MDES so that they can host the tokens for the virtual cards of Mastercard's thousands of United States banks on their wallets. Mastercard has granted such access to the likes of Apple, Samsung, Google, LG, and Garmin for their respective mobile wallets. There are no administrative difficulties with respect to Mastercard doing the same for OV Loop. As described above, Mastercard is in the business of doing so, as a token service provider. Nor are there any legitimate business justifications for denying OV Loop MDES access. For example, OV Loop's solution—which is built by well-known payment experts that worked on widely implemented payment features, including Host Card Emulation, and on a mobile wallet Mastercard has certified to MDES, Samsung Pay—is just as secure as certified wallets.

237. A further example of Mastercard's anticompetitive conduct comes in the form of it forsaking short-term profits in refusing to deal with OV Loop. OV Loop's solution, for example,

reaches use cases that the mobile wallets Mastercard has certified to MDES cannot, and OV Loop's wallet can drive digital payment adoption in ways the certified wallets cannot. In denying OV Loop, Mastercard is losing interchange fees it would generate through OV Loop's mobile wallet, and it is foregoing an opportunity to grow a business it has identified as important to its bottom line. Moreover, Mastercard is forsaking the procompetitive effects—increased security and thereby lower consumer fraud costs—afforded by its own tokenization service in refusing OV Loop MDES access.

238. Mastercard's refusal to deal with OV Loop is part of a larger anticompetitive enterprise to exclude super-apps from the First Relevant Market. Mastercard refuses OV Loop MDES access to prevent OV Loop from leveraging its payment application into a super-app-alternative rails payment system, through which OV Loop would compete for Mastercard's United States processing revenues and prevent Mastercard's monopolization of the First Relevant Market. Mastercard's conduct violates its duty under Section 2 of the Sherman Act to compete fairly within the United States by not forgoing short term profits for the purpose of blocking competition and attempting to knowingly monopolize with a dangerous probability of success. Mastercard's anticompetitive conduct in the First Relevant Market has had, and continues to have, a substantial impact on interstate commerce.

239. As a direct and proximate result of Mastercard's exclusionary conduct, OV Loop has suffered injury to its business, including through hinderance of its full-scale deployment of the OV Super-App and OV Valet, which has resulted in lost profits and lost opportunities, for example. Mastercard's anticompetitive conduct has drastically limited OV Loop's ability to earn revenue and gain traction as a mobile wallet and super-app. OV Loop has suffered damage in an amount to be determined at trial.

240. OV Loop's injury is the type of injury the antitrust laws were designed to prevent and flows from that which makes Mastercard's conduct unlawful. Mastercard's attempts to monopolize, with a dangerous probability of success through its exclusionary acts, have caused substantial anticompetitive effects in the First Relevant Market, including increased consumer costs. OV Loop's suffered injuries are both injuries-in-fact and antitrust injuries and stem directly from Mastercard's refusal to deal with OV Loop. The injury Mastercard has caused and continues to cause OV Loop is a foreseeable consequence of Mastercard's anticompetitive and unlawful conduct.

241. As a result of Mastercard's anticompetitive conduct, OV Loop has been damaged, and will continue to be damaged, until Mastercard is enjoined from discriminating against OV Loop based on Mastercard's anticompetitive intent. Mastercard, to the detriment of competition and the United States consumer and with a dangerous probability of success, has attempted to, and if not restrained by this Court will continue to attempt to, monopolize the First Relevant Market.

242. Mastercard will continue its anticompetitive conduct, which is directed towards OV Loop as well as similar companies posing a competitive threat to Mastercard's attempt to secure monopoly power over transactional fees, and harms competition in the First Relevant Market and consumers, unless enjoined by this Court. OV Loop faces real, substantial, and irreparable damage and injury of a continuing nature, as does competition in the First Relevant Market, from Mastercard's refusal to allow OV Loop access to MDES similar in kind to that which it provides the likes of Apple, Samsung, Google, and Garmin. OV Loop has no adequate remedy at law for this damage.

CLAIM III:
(Violation of Section 2 of the Sherman Act:
Unlawful Monopolization Through Denial of Access to an Essential Facility)

243. OV Loop realleges and incorporates by reference the allegations set forth in the paragraphs above.

244. Mastercard has engaged in conduct violative of Section 2 of the Sherman Act, which "prohibits the "monopoliz[ation of] any part of the trade or commerce among the several States, or with foreign nations." 15 U.S.C. § 2.

245. As described above, Mastercard possesses monopoly power in the First Relevant Market. Mastercard has possessed this monopoly power at all times with respect to the conduct complained of herein.

246. In violation of Section 2 of the Sherman Act, Mastercard has willfully acquired, maintained, and/or continues to maintain its monopoly power in the First Relevant Market, as distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident. Put differently, Mastercard has engaged in and continues to engage in exclusionary, anticompetitive conduct.

247. The anticompetitive conduct at issue is Mastercard's denial of OV Loop's access to MDES—an essential facility that Mastercard controls with anticompetitive malice. MDES is an essential facility with respect to participation in the First Relevant Market.

248. Mastercard is the TSP for its branded virtual cards. As such, Mastercard is the gatekeeper for the tokens of the thousands of United States issuing banks that offer virtual Mastercard branded credit and debit cards. At the heart of Mastercard's tokenization service is MDES, the tokenization infrastructure owned and controlled by Mastercard. If a mobile wallet wants to work with Mastercard branded cards it must be able to access MDES for tokens and

authorization services.

249. Without MDES, OV Loop is functionally unable to operate as a mobile wallet and is thus, badly handicapped as a super-app. Consumers want to be able to use the credit and debit cards they already have. For this reason, all the major mobile wallets have sought (and received) certification to MDES, allowing them to service the customers (consumers) of Mastercard's thousands of United States banks. To be able to gain meaningful traction in the United States market, and thereby offer a super-app-alternative rails payment option to consumers, a super-app's mobile wallet feature must be able to facilitate payments using Mastercard branded debit and credit cards. Since MDES access is the only way OV Loop can do this, MDES is essential to OV Loop's ability to effectively and meaningfully compete, not just with the likes of Apple Pay, but Mastercard itself.

250. It would be economically infeasible for OV Loop to duplicate MDES. OV Loop is unable, reasonably or practically to duplicate MDES. To replicate MDES, OV Loop would have to become the TSP for thousands of United States banks for Mastercard's own cards. A decade into tokenization, the structural barriers and capital expenditures of competing with Mastercard as a TSP for Mastercard's own cards with thousands of banks are too high.

251. Mastercard, with the intent to destroy OV Loop's ability to compete with Mastercard, and with no legitimate business justifications or procompetitive benefits, refuses to provide OV Loop access to MDES. Mastercard has denied OV Loop MDES access because Mastercard fears OV Loop as a competitor in the First Relevant Market. There is no rational explanation for Mastercard's conduct, absent Mastercard's specific intent to harm competition and achieve an anticompetitive effect. Mastercard's intent is to limit OV Loop's ability to gain traction as a super-app and thereby prevent OV Loop from offering a solution, a super-app-alternative

network payment system, that will compete directly with Mastercard's virtual card-card network payment system and through which OV Loop will compete for Mastercard's United States processing revenues. Mastercard has acted to hamstring OV Loop so that Mastercard can reap supracompetitive profits, including profits from processing fees. Mastercard has achieved its aims and continues to achieve its aims through its denial of access to MDES, which prevents the development of a competing super-app-alternative network payment system and maintains Mastercard's supracompetitive fees.

252. It is feasible for Mastercard to provide OV Loop with MDES access. There are no administrative difficulties with respect to Mastercard doing for OV Loop what it has done for other mobile wallet providers, including Apple, Samsung, Google, LG, and Garmin. As described above, Mastercard, as a token service provider, is in the business of providing access to MDES. Nor are there any legitimate business justifications for denying OV Loop MDES access. For example, OV Loop's solution—which is built by well-known payment experts that worked on widely implemented payment features, including Host Card Emulation, and on a mobile wallet Mastercard has certified to MDES, Samsung Pay—is just as secure as certified wallets.

253. More, from both a short-term profit and security perspective, it would benefit Mastercard to provide OV Loop with MDES access. OV Loop's solution, for example, reaches use cases that the mobile wallets Mastercard has certified to MDES cannot, and OV Loop's wallet can drive digital payment adoption in ways the certified wallets cannot. In denying OV Loop MDES access, Mastercard is losing interchange fees it would generate through OV Loop's mobile wallet, and is foregoing an opportunity to grow a business it has identified as important to its bottom line. Additionally, Mastercard is forsaking the procompetitive effects—increased security and thereby lower consumer fraud costs—afforded by its own tokenization service in denying OV

Loop access to MDES.

254. Mastercard has willfully and wrongfully acquired, maintained, and/or maintains its monopoly in the First Relevant Market by denying OV Loop access to MDES, an essential facility. This anticompetitive conduct has had, and continues to have, a substantial impact on interstate commerce, in violation of Section 2 of the Sherman Act.

255. As a direct and proximate result of Mastercard's exclusionary conduct, OV Loop has suffered injury to its business, including through hinderance of its full-scale deployment of the OV Super-App and OV Valet, which has resulted in lost profits and lost opportunities, for example. Mastercard's anticompetitive conduct has drastically limited OV Loop's ability to earn revenue and gain traction as a mobile wallet and super-app. OV Loop has suffered damage in an amount to be determined at trial.

256. OV Loop's injury is the type of injury the antitrust laws were designed to prevent and flows from that which makes Mastercard's conduct unlawful. Mastercard's exclusionary acts and acquisition and/or maintenance of its monopoly have caused substantial anticompetitive effects in the First Relevant Market, including increased consumer costs. OV Loop's suffered injuries are both injuries-in-fact and antitrust injuries, and stem directly from Mastercard's denial of OV Loop access to MDES. The injury Mastercard has caused and continues to cause OV Loop is a foreseeable consequence of Mastercard's anticompetitive and unlawful conduct.

257. As a result of Mastercard's anticompetitive conduct, OV Loop has been damaged, and will continue to be damaged, until Mastercard is enjoined from denying OV Loop access to MDES based on Mastercard's anticompetitive intent. Mastercard has acquired and has maintained, and if not restrained by this Court will continue to maintain, its monopoly power in the First Relevant Market to the detriment of competition and the United States consumer.

258. Mastercard will continue its anticompetitive conduct, which is directed towards OV Loop as well as similar companies posing a competitive threat to Mastercard's monopoly power over transactional fees, and harms competition in the First Relevant Market and consumers, unless enjoined by this Court. OV Loop faces real, substantial, and irreparable damage and injury of a continuing nature, as does competition in the First Relevant Market, from Mastercard's denying OV Loop access to MDES similar in kind to that which it provides the likes of Apple, Samsung, Google, and Garmin. OV Loop has no adequate remedy at law for this damage.

CLAIM IV
(Violation of Section 2 of the Sherman Act:
Attempt to Monopolize by Denial of Access to an Essential Facility)

259. OV Loop realleges and incorporates by reference the allegations set forth in the paragraphs above.

260. In violation of Section 2 of the Sherman Act, Mastercard has attempted to, and is continuing to attempt to, willfully and wrongfully acquire and possess monopoly power in the First Relevant Market. Mastercard has engaged in exclusionary, anticompetitive conduct with the specific intent to monopolize the First Relevant Market with a dangerous probability of achieving monopoly power in said market.

261. Mastercard possesses a dangerous probability of achieving monopoly power in the First Relevant Market. For example: Mastercard commands a substantial share of the First Relevant Market; has been found to have engaged in anticompetitive conduct in other payments network processing services markets; benefits from network effects that it leverages through its control over the tokens for thousands of banks to keep competitors out of the First Relevant Market; has been able to impose higher margin fees in the First Relevant Market without losing market share; and is attempting to monopolize a market with significant barriers to entry.

Mastercard's scheme to monopolize the First Relevant Market has had success in foreclosing competition, and Mastercard has possessed the dangerous probability of achieving monopoly power at all times with respect to the conduct complained of herein.

262. The anticompetitive conduct at issue is Mastercard's denying OV Loop access to MDES—an essential facility that Mastercard controls with anticompetitive malice. MDES is an essential facility with respect to participation in the First Relevant Market.

263. Mastercard is the TSP for its branded virtual cards. As such, Mastercard is the gatekeeper for the tokens of the thousands of United States issuing banks that offer virtual Mastercard branded credit and debit cards. At the heart of Mastercard's tokenization service is MDES, the tokenization infrastructure owned and controlled by Mastercard. If a mobile wallet wants to work with Mastercard branded cards it must be able to access MDES for tokens and authorization services.

264. Without MDES, OV Loop is functionally unable to operate as a mobile wallet and is thus badly handicapped as a super-app. Consumers want to be able to use the credit and debit cards they already have. For this reason, all the major mobile wallets have sought (and received) certification to MDES, allowing them to service the customers (consumers) of Mastercard's thousands of United States banks. To be able to gain meaningful traction in the United States market, and thereby offer a super-app-alternative rails payment option to consumers, a super-app's mobile wallet feature must be able to facilitate payments using Mastercard branded debit and credit cards. Since MDES access is the only way OV Loop can do this, MDES is essential to OV Loop's ability to effectively and meaningfully compete, not just with the likes of Apple Pay, but Mastercard itself.

265. It would be economically infeasible for OV Loop to duplicate MDES. OV Loop is unable, reasonably or practically to duplicate MDES. To replicate MDES, OV Loop would have to become the TSP for thousands of United States banks for Mastercard's own cards. A decade into tokenization, the structural barriers and capital expenditures of competing with Mastercard as a TSP for Mastercard's own cards with thousands of banks are too high.

266. Mastercard, with the intent to destroy OV Loop's ability to compete with Mastercard, and with no legitimate business justifications or procompetitive benefits, refuses to, and continues to refuse to, provide OV Loop access to MDES. Mastercard has denied OV Loop MDES access because Mastercard fears OV Loop as a competitor in the First Relevant Market. There is no rational explanation for Mastercard's conduct, absent a specific Mastercard intent to harm competition and achieve an anticompetitive effect. Mastercard's intent is to limit OV Loop's ability to gain traction as a super-app and thereby prevent OV Loop from offering a solution, a super-app-alternative network payment system, that will prevent Mastercard from establishing a monopoly through direct competition with Mastercard's virtual card-card network payment system and through which OV Loop will compete for Mastercard's United States processing revenues. Mastercard has acted to hamstring OV Loop so that Mastercard can reap supracompetitive profits, including profits from processing fees. Mastercard's continued denial of OV Loop MDES access affords Mastercard a dangerous probability of achieving its aims, the monopolization of the First Relevant Market.

267. It is feasible for Mastercard to provide OV Loop with MDES access. There are no administrative difficulties with respect to Mastercard doing for OV Loop what it has done for other mobile wallet providers, including Apple, Samsung, Google, LG, and Garmin. As described above, Mastercard, as a token service provider, is in the business of providing access to MDES.

Nor are there any legitimate business justifications for denying OV Loop MDES access. For example, OV Loop's solution—which is built by well-known payment experts that worked on widely implemented payment features, including Host Card Emulation, and on a mobile wallet Mastercard has certified to MDES, Samsung Pay—is just as secure as certified wallets.

268. Moreover, from both a short-term profit and security perspective, it would benefit Mastercard to provide OV Loop with MDES access. OV Loop's solution, for example, reaches use cases that the mobile wallets Mastercard has certified to MDES cannot, and OV Loop's wallet can drive digital payment adoption in ways the certified wallets cannot. In denying OV Loop, Mastercard is losing interchange fees it would generate through OV Loop's mobile wallet, and is foregoing an opportunity to grow a business it has identified as important to its bottom line. Additionally, Mastercard is forsaking the procompetitive effects—increased security and thereby lower consumer fraud costs—afforded by its own tokenization service in denying OV Loop access to MDES.

269. Mastercard has, knowing it has a dangerous probability of success, willfully attempted to, and continues to attempt to, monopolize the First Relevant Market by denying OV Loop access to MDES, an essential facility. This anticompetitive conduct has had, and continues to have, a substantial impact on interstate commerce, in violation of Section 2 of the Sherman Act.

270. As a direct and proximate result of Mastercard's exclusionary conduct, OV Loop has suffered injury to its business, including through hinderance of its full-scale deployment of the OV Super-App and OV Valet, which has resulted in lost profits and lost opportunities, for example. Mastercard's anticompetitive conduct has drastically limited OV Loop's ability to earn revenue and gain traction as a mobile wallet and super-app. OV Loop has suffered damage in an amount to be determined at trial.

271. OV Loop's injury is the type of injury the antitrust laws were designed to prevent and flows from that which makes Mastercard's conduct unlawful. Mastercard's attempts to monopolize with a dangerous probability of success through its exclusionary acts have caused substantial anticompetitive effects in the First Relevant Market, including increased consumer costs. OV Loop's suffered injuries are both injuries-in-fact and antitrust injuries and stem directly from Mastercard's denial of OV Loop access to MDES. The injury Mastercard has caused and continues to cause OV Loop is a foreseeable consequence of Mastercard's anticompetitive and unlawful conduct.

272. As a result of Mastercard's anticompetitive conduct, OV Loop has been damaged, and will continue to be damaged, until Mastercard is enjoined from denying OV Loop access to MDES based on Mastercard's anticompetitive intent. Mastercard, to the detriment of competition and the United States consumer and with a dangerous probability of success, has attempted to, and if not restrained by this Court, will continue to attempt to, monopolize the First Relevant Market.

273. Mastercard will continue its anticompetitive conduct, which is directed towards OV Loop as well as similar companies posing a competitive threat to Mastercard's attempt to secure monopoly power over transactional fees, and harms competition in the First Relevant Market and consumers, unless enjoined by this Court. OV Loop faces real, substantial, and irreparable damage and injury of a continuing nature, as does competition in the First Relevant Market, from Mastercard's denying OV Loop access to MDES similar in kind to that which it provides the likes of Apple, Samsung, Google, and Garmin. OV Loop has no adequate remedy at law for this damage.

COUNT V
(Violation of Section 2 of the Sherman Act: Unlawful Monopoly Maintenance)

274. OV Loop realleges and incorporates by reference the allegations set forth in the paragraphs above.

275. Mastercard's conduct violates Section 2 of the Sherman Act, which prohibits the "monopoliz[ation of] any part of the trade or commerce among the several States, or with foreign nations". 15 U.S.C. § 2.

276. The First Relevant Market and Second Relevant Market (collectively, "Relevant Markets") are valid antitrust markets in which Mastercard holds monopoly power.

277. Mastercard has unlawfully maintained monopoly power in the Relevant Markets through the anti-competitive acts, including exclusively providing MDES certification to mobile wallets that do not pose any threat to Mastercard's ability to charge supracompetitive transaction fees, such as its interchange fee. Mastercard has done this by representing that MDES certification is granted to any company that satisfies its technical requirements but, in reality, Mastercard only grants such certification to companies which could never threaten its stranglehold on transaction fees associated with the use of its branded cards. By using MDES to exclude companies from the Relevant Markets, Mastercard forecloses any current or potential future competitors that could threaten its ability to charge supracompetitive transaction fees.

278. Mastercard has also engaged in anticompetitive conduct by precluding OV Loop from the Relevant Markets by withholding MDES certification.

279. Mastercard has used its size, influence, power, and wealth to stifle emerging technology companies, such as OV Loop, that threaten its grip over payment processing networks and therefore, its ability to charge supracompetitive fees on each transaction. Mastercard has done

so, in large part, through selective access to its MDES tokenization service, which it provides for mobile wallets like Apple Pay, Google Pay and Samsung Pay, and are required for any company to compete in the mobile wallet space and therefore, the Relevant Markets. Knowing that it has the ability to control access to the Relevant Markets through this certification, Mastercard wields access to MDES like a sword to keep competition out of and maintain its monopoly in the mobile payment processing space.

280. To a normal market participant, Mastercard's use of MDES to prevent new entrants into the mobile wallet and payment space is illogical in the absence of anticompetitive intent, as more mobile wallets would result in more consumers carrying mobile wallets with Mastercard branded cards, increasing usage, and therefore profit, in addition to Mastercard benefiting from higher revenue and margins with mobile wallet transactions than physical card transactions and Apple Pay.

281. Despite the obvious benefit to Mastercard of a competitive mobile wallet market, Mastercard has taken the opposite approach, instead utilizing its monopoly power in the Relevant Markets to prevent new mobile wallet entrants from gaining acceptance by consumers to protect its control over transactional fees associated with each transaction initiated from a mobile wallet.

282. Mastercard is accomplishing its anticompetitive end-goal by denying OV Loop MDES certification which any mobile wallet must have in order to host and facilitate transactions using a Mastercard branded card. While OV Loop offers alternative payment methods – payment methods with far lower transaction fees – its platform is unable to gain acceptance among consumers without the ability to facilitate transactions using Mastercard branded cards as consumers have no interest in a mobile wallet that cannot perform transactions using their preferred payment card. Thus, by denying OV Loop its MDES certification, Mastercard is able to

keep OV Loop, as well as any other mobile wallet offering point-of-sale payment methods with lower transaction fees, from ever gaining traction among consumers and merchants, allowing it to maintain its monopoly power within the Relevant Markets.

283. Mastercard's anticompetitive use of MDES is also intended to limit its card holders to only the select few mobile wallets it has chosen to grant MDES authorization which similarly allows it to maintain its monopoly power within the Relevant Markets.

284. By only allowing mobile wallets with MDES certification to host its cards, Mastercard is able to dictate which mobile wallets its card holders may use, and merchants may accept, thereby allowing Mastercard to control any and all fees associated with mobile payments through its network.

285. More, as MDES is necessary for any mobile wallet to gain acceptance among United States consumers, withholding MDES not only restricts which mobile wallets its card holders may utilize, but also restricts which mobile wallets all card holders can use, as without Mastercard MDES, a mobile wallet will never gain traction and will inevitably be unable to compete with the big three mobile wallet providers: Samsung, Google, and Apple.

286. The restraints that bind Mastercard holders (the consumers) to certain mobile wallet platforms, while excluding those that may offer alternative payment rails at a lower cost within the Relevant Markets, has been concealed from consumers.

287. Mastercard's exclusive access to MDES deprives consumers of the ability to select the mobile wallet of their choosing and requires merchants to accept high and unnecessary transaction fees in connection with each consumer transaction. All of this is simply to protect Mastercard's ability to charge supracompetitive transaction fees on each transaction completed using a mobile wallet, which is threatened by OV Loop.

288. Mastercard's conduct forecloses competition within the mobile wallet industry, and thus the Relevant Markets, and therefore affects a substantial percentage of all consumer transactions in the United States. This implied agreement results in a net restraint on trade such that the anticompetitive effects outweigh the procompetitive benefits.

289. As a result of restricting consumer's choice of mobile wallet to Samsung, Apple, or Google payment platforms, Mastercard is able to continue charging supracompetitive transaction fees for all transactions that occur on these MDES approved mobile wallets.

290. The mobile wallets operated by Samsung, Apple, and Google do not allow for alternative payment rails in addition to card network payment rails utilized by Mastercard, as OV Loop provides. Therefore, because each of the three mobile wallets rely exclusively on card network payment rails, there are no mobile wallets offering additional payment methods with lower fees associated with conducting POS transactions. As a result, the card payment networks have no reason to lower fees associated with mobile wallet transactions and, in fact, have virtually nothing to prevent them from increasing such fees as consumers, who are largely transitioning to mobile wallet payments, have no other payment options available to them as a result of Mastercard's anticompetitive use of its MDES certification to control access to the Relevant Markets.

291. Mastercard is able to control pricing in the Relevant Markets through their control of the supply chain and access to bank tokens required to utilize Mastercard's branded cards on a mobile wallet platform.

292. Unless and until Mastercard is required to grant MDES certification equally among all qualified applicants, the only mobile wallets that will be available to consumers will only utilize payment rails with similar transaction fees to the fees charged by Mastercard.

293. As discussed herein, Mastercard's anticompetitive conduct costs consumers, merchants, and countless others participating in the United States economy billions of dollars collectively on transaction fees simply because Mastercard refuses to grant MDES to mobile wallet providers offering payment rails with lower fees.

294. Thus, by binding its card holders to specific mobile wallets, Mastercard is able to maintain its monopoly power within the Relevant Markets, as consumers are left without any alternative than to continue paying the supercompetitive transaction fees on each purchase or sale.

295. Mastercard's conduct affects a substantial volume of interstate commerce.

296. Mastercard's conduct has substantial anti-competitive effects, including increased prices and costs, reduced innovation and quality of service, and lowered output.

297. As a potential competing payment network and as a mobile wallet provider, OV Loop has been harmed by Mastercard's anti-competitive conduct in a manner that the antitrust laws were intended to prevent. OV Loop has suffered, and continues to suffer, damages and irreparable injury.

COUNT VI

(Violation of Section 2 of the Sherman Act: Unlawful Attempt to Monopolize)

298. OV Loop realleges and incorporates by reference the allegations set forth in the paragraphs above.

299. In violation of Section 2 of the Sherman Act, Mastercard has attempted to, and is continuing to attempt to, willfully and wrongfully acquire and possess monopoly power in the Relevant Markets. Mastercard has engaged in exclusionary, anticompetitive conduct with the specific intent to monopolize the Relevant Markets with a dangerous probability of achieving monopoly power in said market.

300. Mastercard possesses a dangerous probability of achieving monopoly power in the Relevant Markets. For example: Mastercard commands a substantial share of the Relevant Markets; has been found to have engaged in anticompetitive conduct in other payments network processing services markets; benefits from network effects that it leverages through its control over the tokens for thousands of banks to keep competitors out of the Relevant Markets; has been able to impose higher margin fees in the Relevant Markets without losing market share; and is attempting to monopolize a market with significant barriers to entry. Mastercard's scheme to monopolize the Relevant Markets has had success in foreclosing competition, and Mastercard has possessed the dangerous probability of achieving monopoly power at all times with respect to the conduct complained of herein.

301. As a direct and proximate result of Mastercard's anticompetitive conduct, OV Loop has suffered injury to its business, including through hinderance of its full-scale deployment of the OV Super-App and OV Valet, which has resulted in lost profits and lost opportunities, for example. Mastercard's anticompetitive conduct has drastically limited OV Loop's ability to earn revenue and gain traction as a mobile wallet and super-app. OV Loop has suffered damage in an amount to be determined at trial.

302. Further, as explained above, Mastercard's anti-competitive conduct has also harmed competition within the Relevant Markets, consumers, and the United States economy.

IX. PRAYER FOR RELIEF

WHEREFORE, OV Loop demands judgment in its favor and against Mastercard and relief as follows:

303. Judgment in OV Loop's favor and against Mastercard on all causes of action alleged herein;

304. A declaration, adjudication, and decree that Mastercard has committed the violations of the Sherman Act, 15 U.S.C. § 2, complained of herein;

305. An award of all of the damages sustained by OV Loop, in an amount to be proved at trial, to be trebled according to 15 U.S.C. § 15 (and any other applicable statutes or laws);

306. Pursuant to 15 U.S.C. § 26, and any other applicable statutes or laws, the issuance of preliminary and final injunctions enjoining Mastercard, its officers, directors, agents, servants, employees, attorneys, affiliates, divisions, branches, subsidiaries, parents, and those persons in active concert or participation with any of them, and any other person in active concert of participation with them, from continuing the acts herein complained of with respect to the violations of Section 2 of the Sherman Act, and compelling them to promptly provide OV Loop with access to Mastercard's Mastercard Digital Enablement Service similar in kind to that which they provide the likes of Apple, Samsung, Google, and Garmin;

307. An award of OV Loop's cost of suit, including reasonable attorneys' fees, pursuant to 15 U.S.C. §§ 15 and 26 (and any other applicable statutes or laws);

308. Pre-judgment and post-judgment interest on the damages caused to OV Loop by reason of Mastercard's conduct at the maximum legal rates provided by statute or law;

309. An award of OV Loop's costs and disbursements in this civil action, including reasonable attorneys' fees; and

310. Such other relief as this Court may deem just and proper under the circumstances.

X. DEMAND FOR JURY

Under Rule 38(b) of the Federal Rules of Civil Procedure, OV Loop respectfully requests a trial by jury on all causes of action, claims, and/or issues so triable.

February 21, 2024

Respectfully submitted,

By: */s/ Lawrence G. Green*

Lawrence G. Green (BBO #209060)
lgreen@burnslev.com
Gregory S. Paonessa (BBO #691216)
gpaonessa@burnslev.com
BURNS & LEVINSON LLP
125 High Street
Boston, Massachusetts 02110
Tel: (617) 345-3000 T
Fax: (617) 345-3299 F

Edward T. Kang (to be admitted *Pro Hac Vice*)
Kandis L. Kovalsky (to be admitted *Pro Hac Vice*)
Ross M. Wolfe (to be admitted *Pro Hac Vice*)
KANG HAGGERTY LLC
123 South Broad Street, Suite 1950
Philadelphia, Pennsylvania 19109
(215) 525-5850 (tel)
(215) 525-5860 (fax)
ekang@kanghaggerty.com
kkovalsky@kanghaggerty.com
rwolfe@kanghaggerty.com

Oliver Griffin (to be admitted *Pro Hac Vice*)
Peter Kessler (to be admitted *Pro Hac Vice*)
GRIFFIN PARTNERS LLP
123 South Broad Street, Suite 1850
Philadelphia, Pennsylvania 19109
Tel: (267) 313-0766
Fax: (267) 427-8139
oliver.griffin@griffinlawllp.com
peter.kessler@griffinlawllp.com

Attorneys for Plaintiff OV LOOP, INC.